Universidade Federal de Santa Catarina
Curso de Pós-Graduação em Matemática e
Computação Científica

Teorema Chinês de Restos e Teorema da Aproximação

Graziela de Souza Sombrio
Orientador: Prof. Dr. Oscar Ricardo Janesch

Florianópolis
Maio de 2001

Universidade Federal de Santa Catarina
Curso de Pós-Graduação em Matemática e Computação Científica

Teorema Chinês de Restos e Teorema da Aproximação

Dissertação apresentada ao Curso de Pós-Graduação em Matemática e Computação Científica, do Centro de Ciências Físicas e Matemáticas da Universidade Federal de Santa Catarina, para a obtenção do grau de Mestre em Matemática, com Área de Concentração em Álgebra.

Graziela de Souza Sombrio
Florianópolis
Maio de 2001

Teorema Chinês de Restos e Teorema da Aproximação

por

Graziela de Souza Sombrio

Esta Dissertação foi julgada para a obtenção, do Título de "Mestre", Área de Concentração em Álgebra, e aprovada em sua forma final pelo Curso de Pós-Graduação em Matemática e Computação Científica.

Celso Melchíades Dória
Coordenador

Comissão Examinadora

Prof. Dr. Oscar Ricardo Janesch (UFSC-Orientador)

Prof. Dr. Alveri Alves Sant'Ana (UFRGS)

Prof. Dra. Albertina Zatelli (UFSC)

Prof. Dr. Celso Melchíades Dória (UFSC)

Florianópolis, maio de 2001.

Aos meus pais

Agradecimentos

Agradeço ao meu namorado, Márcio, e a minha família, pelo incentivo dado em todos os momentos.

Aos meus colegas de Graduação e Pós-Graduação Airton, Anderson, Andresa, Christian, Claiton, Danilo, Daniel, Dirceu, Fábio, Janice, Juliano, Maria Inez, Milton, Patrícia, Paulo e Rafael pela amizade e agradável companhia.

Aos professores, Carmen, Pinho, Ruy Exel e William pelos conhecimentos repassados e pela amizade, e aos funcionários, Alcino, Elisa, Iara e Silvia, pela amizade durante os períodos de Graduação e Pós-Graduação.

À CAPES, pelo auxílio financeiro recebido.

Meu especial agradecimento ao meu orientador Oscar Ricardo Janesch, pelo apoio e amizade.

Resumo

O principal objetivo deste trabalho é demonstrar o Teorema da Aproximação para anéis de valorização. Inicialmente demonstramos o Teorema Chinês de Restos, o qual é equivalente ao Teorema da Aproximação para anéis.

O Teorema da Aproximação é estudados sob vários aspectos e obtemos versões deste para valores absolutos, valorizações exponenciais e anéis de valorização.

Sumário

Introdução

O Teorema Chinês de Restos, bem como vários outros assuntos estudados em Matemática, surgiram a partir de algum problema prático. Este em particular, envolve apenas o anel dos inteiros, o que leva a formular o Teorema Chinês de Restos para um anel comutativo qualquer. Essa formulação será nossa primeira versão do Teorema Chinês de Restos e terá, como caso particular, o Teorema Chinês de Restos para o anel $\mathbb{Z}$.

Particularizando a primeira versão do Teorema Chinês de Restos, mostraremos que tal Teorema possui várias outras formulações que envolvem diferentes conceitos em álgebra. Mesmo assim, tais formulações não são necessariamente equivalentes.

Uma aplicação do Teorema Chinês de Restos é no cálculo da função de Euler, o que possibilita, entre outros, contar o número de geradores do anel $(\mathbb{Z}_n, +)$. Posteriormente verificaremos que a aritmética de ideais pode ser relacionada com o Teorema Chinês de Restos, bem como os conceitos de domínios principais e anéis aritméticos.

O Teorema da Aproximação para valores absolutos surge para substituir o Teorema Chinês de Restos quando passamos a trababalhar com corpos ao invés de anéis. Veremos uma aplicação importante deste Teorema, a qual permite construir ordens para um corpo.

Os valores absolutos de um corpo $\mathbb{K}$ são eficientes para tornar $\mathbb{K}$ um corpo topológico. A partir disso e de alguns resultados sobre corpos topológicos, podemos

mostrar uma versão topológica do Teorema da Aproximação visto anteriormente.

Os valores absolutos podem ser classificados em arquimedianos e não-arquimedianos. Estes últimos dão origem às valorizações exponenciais, as quais podem ser consideradas equivalentes quando são geradas por valores absolutos equivalentes. Obtemos então um resultado importante, o Teorema da Aproximação para valorizações exponenciais.

As valorizações exponenciais podem ainda ser generalizadas, definindo assim, as valorizações de Krull. Antes de fazermos tal generalização, estudaremos um pouco sobre anéis de valorização de um corpo e suas propriedades, para podermos relacioná-los com as valorizações de Krull deste corpo.

Outro conceito importante é o de anel de Prüfer. Esse, juntamente com o Teorema Chinês de Restos visto no início do trabalho, permitem-nos demonstrar o Teorema da Aproximação para os anéis de valorização.

Neste trabalho iremos nos referir sempre a anéis comutativos e com unidade.

Capítulo 1

Teorema Chinês de Restos

Na primeira seção deste capítulo apresentamos duas formulações do Teorema Chinês de Restos, que caracterizam os sistemas de congruências lineares de um anel comutativo com unidade que possuem solução. Uma particularização destes Teoremas ao anel $\mathbb{Z}$ possibilita explicitar a solução de tais sistemas. Na segunda seção provamos o Teorema Chinês de Restos para sistemas de congruências que envolvem potências de ideais. Provamos também o Teorema Chinês de Restos para módulos, para domínios de Dedekind, e mostramos a versão usual do Teorema Chinês de Restos em teoria de anéis. Na seção seguinte usamos o Teorema Chinês de Restos para provar propriedades da função de Euler, que são usadas para contar o número de geradores do grupo $(\mathbb{Z}_n, +)$, e também para determinar a ordem do grupo multiplicativo dos elementos inversíveis do anel $(\mathbb{Z}_n, +, \cdot)$, e o número de raízes n-ésimas primitivas da unidade em um corpo qualquer. Dedicamos a última seção do capítulo ao estudo de propriedades aritméticas dos ideais de um anel comutativo com unidade. O principal resultado desta seção, assegura que a distributividade da soma de ideais em relação a interseção, e vice-versa, está relacionado com o Teorema Chinês de Restos.

1.1 O Teorema Chinês de Restos

Uma formulação simples do Teorema Chinês de Restos assegura que dados $p_1, \cdots, p_n$ primos distintos e $a_1, \cdots, a_n$ inteiros, existe um inteiro x tal que p_i divide $x - a_i$, para $i = 1, \cdots, n$. De outra forma, a_i é o resto da divisão de x por p_i para cada $i \in \{1, \cdots, n\}$.

Acredita-se que os chineses anteriores a era cristã já tinham conhecimento deste fato, que possivelmente estava relacionado com um problema prático da época. Contudo, o matemático chinês Sun Tsu (século I d.C.) teve seu nome fortemente associado ao Teorema Chinês de Restos, sendo considerado o divulgador deste resultado. Um registro sobre os trabalhos de Sun Tsu pode ser visto em [23].

O problema específico abordado por Sun Tsu foi obter o menor inteiro positivo que dividido por 3, 5 e 7 tivesse restos 2, 3 e 2, respectivamente. Curiosamente, conta Emil Grosswald ([14], p.48), exatamente o mesmo problema foi abordado pelo Neo-Pitagórico Nicomachus, também do século I d.C..

Um problema semelhante, onde nem todos os divisores são primos, foi formulado e resolvido por Brahmagupta no século VII d.C., que deseja obter um inteiro positivo que dividido por 3, 4, 5 e 6 deixasse restos 2, 3, 4 e 5, respectivamente. Uma discussão sobre o método de resolução de Brahmagupta pode ser encontrado no livro de Le Veque [18], e outras notas históricas podem ser vistas no livro de Dickson [4].

Os problemas estudados por Sun-Tsu e Brahmagupta serão abordados no final desta seção como conseqüência de uma formulação do Teorema Chinês de Restos.

O Teorema Chinês de Restos é usado para obter resultados sobre vários assuntos em Álgebra. Desta forma, o enunciado de tal Teorema varia na literatura segundo o enfoque de cada autor. Estes enunciados não são necessariamente equi-

valentes, mas em geral fornecem condições suficientes para a existência de solução para um sistema de congruências.

Nosso primeiro objetivo é obter uma formulação do Teorema Chinês de Restos para um anel comutativo qualquer ao invés do anel $\mathbb{Z}$. Para isso iniciamos lembrando a definição de congruência módulo um ideal, e fixando algumas notações.

Definição 1.1.1 *Sejam A um anel, I um ideal de A e $a, b \in A$. Dizemos que a é côngruo à b módulo I quando $a - b \in I$.*

Usaremos a notação $a \equiv b \ (mod\ I)$ para indicar que a é côngruo à b módulo I. Quando $A = \mathbb{Z}$ e $I = m\mathbb{Z}$, escrevemos simplesmente $a \equiv b \ (mod\ m)$.

É fácil ver que a relação $a \equiv b \ (mod\ I)$ é uma relação de equivalência em A, e $a \equiv b \ (mod\ I)$ e $c \equiv d \ (mod\ I)$ implica $a + c \equiv b + d \ (mod\ I)$ e $ac \equiv bd \ (mod\ I)$. Isso garante que o conjunto quociente $\frac{A}{I}$ tem estrutura de anel comutativo.

Dados $a, b \in A$, dizemos que a congruência $bx \equiv a \ (mod\ I)$ tem solução em A quando existe $x \in A$ que a satisfaça. Dizemos ainda que a congruência tem solução única módulo I, quando tem solução e quaisquer duas soluções são congruentes módulo I, isto é, existe uma única classe em $\frac{A}{I}$ que a satisfaça. Ilustramos isso através dos seguintes exemplos:

- $2x \equiv 1 \ (mod\ 6)$ não tem solução em $\mathbb{Z}$;
- $2x \equiv 2 \ (mod\ 4)$ tem infinitas soluções em $\mathbb{Z}$ e possiu 2 soluções módulo $4\mathbb{Z}$, a saber as classes $\overline{1}$ e $\overline{3}$ em $\frac{\mathbb{Z}}{4\mathbb{Z}}$;
- $x \equiv 0 \ (mod\ 2)$ tem infinitas soluções em $\mathbb{Z}$ e uma única solução módulo $2\mathbb{Z}$.

O Teorema Chinês de Restos, da forma como foi exposto no início da seção,

garante que o sistema de congruências lineares em $\mathbb{Z}$,

$$\begin{cases} x \equiv a_1 \ (mod\ p_1) \\ x \equiv a_2 \ (mod\ p_2) \\ \quad \vdots \\ x \equiv a_n \ (mod\ p_n) \end{cases},$$

tem solução inteira quando $p_1, \cdots, p_n$ são primos distintos.

Veremos no Corolário 1.1.1 adiante, que basta considerar $m_1, \cdots, m_n$ primos relativos, para obter solução única, módulo $m_1 \cdots m_n$, para um sistema de congruências lineares em $\mathbb{Z}$ da forma,

$$\begin{cases} b_1 x \equiv a_1 \ (mod\ m_1) \\ b_2 x \equiv a_2 \ (mod\ m_2) \\ \quad \vdots \\ b_n x \equiv a_n \ (mod\ m_n) \end{cases}, \tag{1.1}$$

quando m_i é primo relativo com b_i, para $i = 1, 2, \cdots, n$.

Para um anel comutativo A, o Teorema Chinês de Restos assegura a existência de solução para um sistema de congruências em A, cujas variáveis são normalmente assumidas com coeficientes todos iguais a 1. Trabalharemos sem esta restrição, e veremos que as dificuldades podem ser contornadas através de propriedades aritméticas dos ideais de A. Para tal, consideraremos A um anel comutativo com unidade.

Sejam $I_1, \cdots, I_n$ ideais do anel A e $a_1, \cdots, a_n, b_1, \cdots, b_n \in A$. Para estudar um

sistema de congruências em A da forma

$$\begin{cases} b_1 x \equiv a_1 \ (mod\ I_1) \\ b_2 x \equiv a_2 \ (mod\ I_2) \\ \quad \vdots \\ b_n x \equiv a_n \ (mod\ I_n) \end{cases},$$

precisamos saber inicialmente quando cada congruência tem solução. É claro que $b_i \in U(A)$ é condição suficiente para obtermos solução para $b_i x \equiv a_i \ (mod\ I_i)$, porém esta condição não é necessária, como veremos no exemplo $2x \equiv 2 \ (mod\ 4)$ que tem solução em $\mathbb{Z}$.

Quando A é um domínio principal e $I = < m >$ é um ideal de A, é fácil ver que a existência de solução para a congruência $bx \equiv a \ (mod\ I)$ é equivalente a existência de solução para a equação diofantina $bX + mY = a$. E isso ocorre exatamente quando $a \in < b > + < m > = < b > + I$. Este resultado motiva o Lema que veremos a seguir, o qual trabalha com um anel comutativo qualquer.

Note ainda que a existência da Identidade de Bezout nos domínios principais assegura que $a \in < b > + < m >$ se, e somente se, $mdc(b, m) \mid a$. Assim, para domínios principais, $bx \equiv a \ (mod \ < m >)$ (ou equivalentemente $bX + mY = a$) tem solução se, e somente se, $mdc(b, m) \mid a$.

Lema 1.1.1 *Sejam A um anel, I um ideal de A e $a, b \in I$. São equivalentes:*

(i) A congruência $bx \equiv a \ (mod\ I)$ tem solução em A;

(ii) $a \in I + < b >$.

Quando $I + < b > = A$ então a congruência acima tem solução única módulo I.

Demonstração: A congruência $bx \equiv a \ (mod\ I)$ tem solução em A se, e somente se, existe $\alpha \in A$ tal que $b\alpha - a \in I$. Chamando $b\alpha - a = -u \in I$, vemos que (i) é equivalente a existir $\alpha \in A$ tal que $a = b\alpha + u \in < b > + I$. Assumimos agora que

$I + < b > = A$, e então, por $(ii) \Rightarrow (i)$, a congruência $bx \equiv a \ (mod\ I)$ tem solução. Se $x_0, x_1 \in A$ são soluções temos que $bx_0 \equiv bx_1 \ (mod\ I)$, isto é, $b(x_0 - x_1) \in I$. Nossa hipótese assegura que existem $\beta \in A$ e $v \in I$ tais que $1 = v + \beta b$. Como $\beta b(x_0 - x_1) \in I$ concluímos que $(1 - v)(x_0 - x_1) = (x_0 - x_1) + v(x_1 - x_0) \in I$. Portanto, $x_0 - x_1 \in I$, ou seja, $x_0 \equiv x_1 \ (mod\ I)$.

■

A existência de solução para cada uma das congruências de um sistema não garante a existência de solução para o sistema, como pode ser observado em

$$\begin{cases} 2x \equiv 2 \ (mod\ 4) \\ x \equiv 0 \ (mod\ 2) \end{cases}.$$

Desta forma, precisamos impor outras condições para obter solução de um sistema de congruências.

Analisando o sistema acima, podemos entender porque não há solução. De fato, a congruência $x \equiv 0 \ (mod\ 2)$ é equivalente a $2x \equiv 0 \ (mod\ 4)$, que é incompatível com a primeira congruência do sistema.

Em um domínio principal A, este tipo de incompatibilidade poderá ocorrer no sistema

$$\begin{cases} b_1 x \equiv a_1 \ (mod\ I_1) \\ b_2 x \equiv a_2 \ (mod\ I_2) \end{cases},$$

com $I_1 = < m_1 >$ e $I_2 = < m_2 >$, quando $m_1 \mid m_2$ ou $m_2 \mid m_1$. Uma forma para evitar isso é exigir que $mdc(m_1, m_2) = 1$, que pela Identidade de Bezout, equivale a $A = I_1 + I_2$.

Veremos adiante que a condição de comaximalidade, $I_1 + I_2 = A$, é suficiente para obter solução para o sistema acima, quando cada congruência tem solução. Mais do que isso, este resultado se estenderá a um sistema com n congruências em um anel comutativo qualquer. No caso em que $n = 2$ e os coeficientes das variáveis

são iguais a 1, temos a seguinte caracterização dos sistemas de congruência que têm solução, independente da comaximalidade.

Proposição 1.1.1 *Sejam I_1 e I_2 ideais de A e $a_1, a_2 \in A$. São equivalentes:*

(i) $\begin{cases} x \equiv a_1 \ (mod\ I_1) \\ x \equiv a_2 \ (mod\ I_2) \end{cases}$, *tem solução;*

(ii) $a_1 \equiv a_2 \ (mod\ I_1 + I_2)$.

Demonstração:

$(i) \Rightarrow (ii)$ Se $x \in A$ é solução do sistema então $x - a_1 \in I_1$ e $x - a_2 \in I_2$. Segue que $a_1 - a_2 = (x - a_2) - (x - a_1) \in I_1 + I_2$.

$(ii) \Rightarrow (i)$ Por hipótese, existem $c_1 \in I_1$ e $c_2 \in I_2$ tais que $a_1 - a_2 = c_1 + c_2$. Tome $x = a_1 - c_1 = a_2 + c_2$.

■

A condição de comaximalidade restringe o tipo de sistemas que abordamos. No entanto, é nesta situação que o Teorema Chinês de Restos é formulado, pois a comaximalidade de I_1 e I_2 é uma condição necessária para que o sistema

$$\begin{cases} x \equiv 1 \ (mod\ I_1) \\ x \equiv 0 \ (mod\ I_2) \end{cases}$$

tenha solução, como pode ser visto aplicando a Proposição 1.1.1.

Para demonstrar o Teorema Chinês de Restos, provaremos primeiro um Lema, cujo enunciado envolve produto de ideais. Lembramos que se I e J são ideais de A então

$$I \cdot J = \{\sum_{i=1}^{n} x_i y_i; n \in \mathbb{N}, x_i \in I, y_i \in J\}$$

é um ideal de A e $I \cdot J \subseteq I \cap J$. Entretanto, a outra inclusão nem sempre é verdadeira. Basta observar que para $A = \mathbb{Z}$, $I = < x >$ e $J = < y >$ temos $I \cap J = < m >$ onde $m = mmc(x, y)$ e $I \cdot J = < xy >$, portanto $I \cap J = I \cdot J$ se e

somente se $mdc(x,y) = 1$. Em particular, tomando $I = <2>$ e $J = <4>$ temos $I \cdot J = <8> \subsetneq <4> = I \cap J$. A noção de produto de uma quantidade finita de ideais é análoga.

Quando $A = I + J$ é fácil ver que $I \cap J = I \cdot J$, pois dado $x \in I \cap J$ usamos o fato de $1 = \alpha + \beta$, com $\alpha \in I$ e $\beta \in J$, para obter $x = \alpha x + \beta x \in I \cdot J$. A recíproca da implicação acima não é verdadeira, como podemos ver tomando $A = \mathbb{Z}_{12}$, $I = <\overline{2}>$ e $J = <\overline{4}>$ onde $I \cdot J = J = I \cap J$ porém, $I + J = I \neq A$.

Observamos ainda que se I e J são ideais do anel A, então a inclusão $I \cdot J \subseteq I \cap J$ garante que congruência módulo $I \cdot J$ implica em congruência módulo I e congruência módulo J. Assim, solução única módulo $I \cdot J$ assegura solução única módulo I e também módulo J.

Lema 1.1.2 *Sejam $I_1, \cdots, I_n$ ideais do anel A tais que $I_i + I_j = A$ para $i \neq j$. Então:*

(a) *Para cada $i \in \{1, \cdots, n\}$, temos que $I_i + (I_1 \cdots I_{i-1} \cdot I_{i+1} \cdots I_n) = A$;*

(b) $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$.

Demonstração:

(a) Fixe i. Para cada $j \neq i$ existem, por hipótese, $a_j \in I_i$ e $b_j \in I_j$ tais que $a_j + b_j = 1$, e então $1 = \prod_{\substack{j=1 \\ j \neq i}}^{n} (a_j + b_j)$. Desenvolvendo este produtório obtemos uma parcela $b_1 \cdots b_{i-1} \cdot b_{i+1} \cdots b_n \in I_1 \cdots I_{i-1} \cdot I_{i+1} \cdots I_n$, e todas as demais parcelas são produtos que envolvem um fator $a_j \in I_i$. Portanto, $1 \in I_i + (I_1 \cdots I_{i-1} \cdot I_{i+1} \cdots I_n)$ e assim, $I_i + (I_1 \cdots I_{i-1} \cdot I_{i+1} \cdots I_n) = A$.

(b) Faremos por indução sobre n. Quando $n = 2$ temos $I_1 + I_2 = A$, e já vimos que neste caso $I_1 \cdot I_2 = I_1 \cap I_2$. Suponha que $I_1 \cdots I_{n-1} = I_1 \cap \cdots \cap I_{n-1}$, quando os ideais são dois a dois comaximais. Considere agora uma família $I_1, \cdots, I_n$ de ideais dois a dois comaximais. Pelo item (a) vemos que I_n e $I_1 \cdots I_{n-1}$ são comaximais.

Assim, $I_1 \cdots I_{n-1} \cdot I_n = (I_1 \cdots I_{n-1}) \cap I_n = I_1 \cap \cdots \cap I_{n-1} \cap I_n$.

■

Em particular, o Lema anterior assegura que se $I_1, \cdots, I_n$ são ideais de A então $I_i + I_j = A$, para $i \neq j$ se e somente se $I_i + \bigcap_{\substack{j=1 \\ j \neq i}}^{n} I_j = A$.

No Teorema abaixo veremos que a existência de solução para cada congruência de um sistema garante a existência de solução para este sistema, quando os ideais envolvidos são dois a dois comaximais.

Teorema 1.1.1 (Teorema Chinês de Restos) *Sejam A um anel, $a_1, \cdots, a_n$, $b_1, \cdots, b_n \in A$ e $I_1, \cdots, I_n$ ideais de A tais que $I_i + I_j = A$ para $i \neq j$. São equivalentes:*

(*i*) *O sistema*

$$\begin{cases} b_1 x \equiv a_1 \ (mod\ I_1) \\ \quad \vdots \\ b_n x \equiv a_n \ (mod\ I_n) \end{cases}, \tag{1.2}$$

tem solução em A;

(*ii*) $a_i \in I_i + < b_i >$ *para cada* $i \in \{1, \cdots, n\}$.

Além disso, se $I_i + < b_i > = A$ para $i \in \{1, \cdots, n\}$ então a solução é única módulo $I_1 \cdots I_n$.

Demonstração:

$(i) \Rightarrow (ii)$ Como o sistema tem solução, cada congruência tem solução. Segue do Lema 1.1.1 que $a_i \in I_i + < b_i >$ para cada $i \in \{1, \cdots, n\}$.

$(ii) \Rightarrow (i)$ Por hipótese temos que $a_i \in I_i + < b_i >$ para cada $i \in \{1, \cdots, n\}$ e aplicando o Lema 1.1.1 temos que existe $c_i \in A$ tal que c_i é solução de $b_i x \equiv a_i \ (mod\ I_i)$, isto é, $b_i c_i - a_i \in I_i$. Como $I_i + I_j = A$ quando $i \neq j$, pelo Lema 1.1.2 item (a), temos que, para cada $i \in \{1, \cdots, n\}$ existem $\lambda_i \in I_i$ e

$t_i \in I_1 \cdots I_{i-1} \cdot I_{i+1} \cdots I_n$ tais que $\lambda_i + t_i = 1$. Consideramos, para cada i, a congruência $t_i y \equiv 1 \ (mod\ I_i)$. Pelo Lema 1.1.1, esta congruência tem solução se e somente se $1 \in I_i + < t_i >$, e isso é verificado, pois vimos que $\lambda_i + t_i = 1$, onde $\lambda_i \in I_i$. Desta forma, obtemos $y_i \in A$ tal que $t_i y_i - 1 \in I_i$. Tomamos

$$x = y_1 c_1 t_1 + \cdots + y_n c_n t_n \in A.$$

Vamos verificar que $b_i x \equiv a_i \ (mod\ I_i)$ para $i \in \{1, \cdots, n\}$. Note que para $j \neq i$ temos que $t_j \in I_i$ pois $t_j \in I_1 \cdots I_{j-1} \cdot I_{j+1} \cdots I_n \subseteq I_i$. Assim,
$b_i y_1 c_1 t_1, \cdots, b_i y_{j-1} c_{j-1} t_{j-1}, b_i y_{j+1} c_{j+1} t_{j+1}, \cdots, b_i y_n c_n t_n \in I_i$. Logo, para ver que $b_i x - a_i \in I_i$, basta mostrarmos que $b_i y_i c_i t_i - a_i \in I_i$. Mas, $t_i y_i - 1 \in I_i$, donde $b_i y_i c_i t_i - b_i c_i \in I_i$, com $b_i c_i - a_i \in I_i$. Segue que $b_i y_i c_i t_i - a_i \in I_i$.
Para provar que a solução é única, módulo $I_1 \cdots I_n$, consideramos x_1 e x_2 soluções do sistema. Por hipótese, $I_i + < b_i > = A$ para $i = 1, \cdots, n$. Então, pela unicidade vista no Lema 1.1.1, $x_1 \equiv x_2 \ (mod\ I_i)$. Desde que $x_1 - x_2 \in I_1 \cap I_2 \cap \cdots \cap I_n$, aplicamos o Lema 1.1.2 item (b) e obtemos $x_1 \equiv x_2 \ (mod\ I_1 \cdots I_n)$.

■

Fazendo $b_1 = \cdots = b_n = 1$ no Teorema anterior, vemos que a condição (ii) se verifica trivialmente. Portanto, o sistema

$$\begin{cases} x \equiv a_1 \ (mod\ I_1) \\ \quad \vdots \\ x \equiv a_n \ (mod\ I_n) \end{cases}$$

sempre tem solução única, módulo $I_1 \cdots I_n$, quando os ideais são dois a dois comaximais.

Observe que a existência de solução para um sistema de congruências da forma

(1.2) não implica na comaximalidade dos ideais $I_1, \cdots, I_n$. Por exemplo, o sistema

$$\begin{cases} 2x \equiv 2 \ (mod\ 4) \\ 3x \equiv 3 \ (mod\ 2) \end{cases},$$

tem todo número ímpar como solução, porém $2\mathbb{Z} + 4\mathbb{Z} \neq \mathbb{Z}$. No entanto, a comaximalidade dois a dois dos ideais $I_1, \cdots, I_n$ é equivalente a solução de todo sistema da forma (1.2), cujas congruências tenham solução. Este é o resultado do próximo Teorema, que também é chamado de Teorema Chinês de Restos.

Teorema 1.1.2 *Sejam $I_1, \cdots, I_n$ ideais do anel A. São equivalentes:*

(*i*) $I_i + I_j = A$ *para* $i \neq j$;

(*ii*) *Para quaisquer* $a_1, \cdots, a_n, b_1, \cdots, b_n \in A$ *com* $a_i \in < b_i > \ + I_i$, $1 \leq i \leq n$, *o sistema*

$$\begin{cases} b_1 x \equiv a_1 \ (mod\ I_1) \\ \quad \vdots \\ b_n x \equiv a_n \ (mod\ I_n) \end{cases}, \tag{1.2}$$

tem solução em A.

Além disso, se valem as condições acima e $< b_i > \ + I_i = A$ *para* $i \in \{1, \cdots, n\}$ *então a solução é única módulo* $I_1 \cdots I_n$.

Demonstração:

(*i*) $\Rightarrow$ (*ii*) Segue da implicação (*ii*) $\Rightarrow$ (*i*) do Teorema 1.1.1.

(*ii*) $\Rightarrow$ (*i*) Dados $i, j \in \{1, \cdots, n\}$ com $i \neq j$ tome $a_i = 1$, $a_k = 0$ para $k \neq i$, $b_i = b_j = 1$ e $b_k = 0$ para $k \neq i$ e $k \neq j$. Assim, $a_l \in < b_l > \ + I_l$ para $l \in \{1, \cdots, n\}$ e, por hipótese, o sistema $\begin{cases} x \equiv 1 \ (mod\ I_i) \\ x \equiv 0 \ (mod\ I_j) \end{cases}$, tem solução. Portanto, existe $\alpha \in A$ tal que $\alpha \in I_j$ e $\alpha - 1 \in I_i$. Chamando $\alpha - 1 = -\beta \in I_i$ temos $1 = \alpha + \beta \in I_j + I_i$, isto é, $I_i + I_j = A$.

A unicidade da solução, quando $< b_i > + I_i = A$, também segue do Teorema 1.1.1.

■

O Teorema anterior pode ser reescrito para o anel $A = \mathbb{Z}$ da seguinte forma:

Corolário 1.1.1 *Sejam $m_1, \cdots, m_n \in \mathbb{Z}$. São equivalentes:*

(*i*) $mdc(m_i, m_j) = 1$ *para* $i \neq j$;

(*ii*) *Para quaisquer* $a_1, \cdots, a_n, b_1, \cdots, b_n \in \mathbb{Z}$ *tais que* $mdc(b_i, m_i) \mid a_i$, $1 \leq i \leq n$, *o sistema*

$$\begin{cases} b_1 x \equiv a_1 \ (mod\ m_1) \\ \quad \vdots \\ b_n x \equiv a_n \ (mod\ m_n) \end{cases}, \tag{1.1}$$

tem solução em $\mathbb{Z}$.

Se vale a equivalência acima e $mdc(b_i, m_i) = 1$ *para* $1 \leq i \leq n$, *então a solução é única módulo* $m_1 \cdots m_n$.

Demonstração: Observe que:

- Dados $i \neq j$ temos que $mdc(m_i, m_j) = 1$ se, e somente se, $m_i\mathbb{Z} + m_j\mathbb{Z} = A$.
- Dado i, com $1 \leq i \leq n$, temos que $mdc(b_i, m_i) \mid a_i$ se, e somente se, $a_i \in < b_i > + m_i\mathbb{Z}$.

Assim, a demonstração segue imediatamente do Teorema 1.1.2.

■

A próxima Proposição é uma formulação do Teorema Chinês de Restos para o anel $\mathbb{Z}$, onde explicitamos a solução do sistema de congruências.

Proposição 1.1.2 *Dados* $a_1, \cdots, a_n, b_1, \cdots, b_n, m_1, \cdots, m_n \in \mathbb{Z}$ *tais que* $mdc(m_i, m_j) = 1$, *para* $i \neq j$. *São equivalentes:*

(*i*) *O sistema*

$$\begin{cases} b_1 x \equiv a_1 \ (mod\ m_1) \\ \quad \vdots \\ b_n x \equiv a_n \ (mod\ m_n) \end{cases}, \tag{1.1}$$

tem solução em $\mathbb{Z}$.

(*ii*) $mdc(b_i, m_i) \mid a_i$ *para* $1 \leq i \leq n$.

Neste caso, uma solução para o sistema (1.1) é

$$x = \sum_{i=1}^{n} y_i c_i t_i \in \mathbb{Z}$$

onde $t_i = m_1 \cdots m_{i-1} \cdot m_{i+1} \cdots m_n$, c_i *é uma solução de* $b_i x \equiv a_i \ (mod\ m_i)$ *e* y_i *é solução de* $t_i y \equiv 1 \ (mod\ m_i)$. *Além disso, se* $mdc(b_i, m_i) = 1$ *para* $1 \leq i \leq n$ *então* x *é a única solução módulo* $m_1 \cdots m_n$.

Demonstração: A equivalência entre as condições (*i*) e (*ii*), bem como a unicidade da solução, são obtidas do Teorema 1.1.1 de forma análoga a que fizemos no Corolário anterior. Assim, basta mostrar que $x = \sum_{i=1}^{n} y_i c_i t_i$, com y_i, c_i e t_i satisfazendo as condições acima, é uma solução. Como $mdc(b_i, m_i) \mid a_i$ temos que $a_i \in < b_i > \ + \ < m_i >$ e segue do Lema 1.1.1 que $b_i x \equiv a_i \ (mod\ m_i)$ tem uma solução $c_i \in \mathbb{Z}$. De $mdc(m_i, m_j) = 1$, para $i \neq j$, e $t_i = m_1 \cdots m_{i-1} \cdot m_{i+1} \cdots m_n$ concluímos que $mdc(t_i, m_i) = 1$, pois se $d = mdc(t_i, m_i)$ e supomos que $d \neq 1$ então existe um número primo p que divide d, assim $p \mid m_i$ e $p \mid m_1 \cdots m_{i-1} \cdot m_{i+1} \cdots m_n$ implicando em $p \mid m_i$ e $p \mid m_j$ para $i \neq j$, que contradiz a hipótese $mdc(m_i, m_j) = 1$ para $i \neq j$. Novamente do Lema 1.1.1 e de $mdc(t_i, m_i) = 1$ podemos garantir que $t_i y \equiv 1 \ (mod\ m_i)$ tem uma solução $y_i \in \mathbb{Z}$. Agora para ver que $x = \sum_{i=1}^{n} y_i c_i t_i$ é solução para (1.1), basta proceder como fizemos na parte final da demonstração do Teorema 1.1.1.

■

Note que a condição $mdc(b_i, m_i) = 1$ para $1 \leq i \leq n$, da Proposição anterior, é essencial para termos a unicidade módulo $m_1 \cdots m_n$, da solução do sistema (1.1). De fato, o sistema

$$\begin{cases} 2x \equiv 4 \ (mod\ 6) \\ x \equiv 2 \ (mod\ 7) \end{cases}$$

satisfaz as condições da Proposição 1.1.2 com excessão de $mdc(b_1, m_1) = 1$ e neste caso $x = 2$ e $x = 23$ são soluções do sistema, mas $2 \not\equiv 23 \ (mod\ 42)$.

Para um sistema de congruências em $\mathbb{Z}$, com coeficientes iguais a 1, isto é, um sistema da forma

$$\begin{cases} x \equiv a_1 \ (mod\ m_1) \\ \quad \vdots \\ x \equiv a_n \ (mod\ m_n) \end{cases},$$

podemos tomar $c_i = a_i$ como solução para a i-ésima linha, obtendo a solução $x = \sum_{i=1}^{n} y_i a_i t_i$.

Para o sistema estudado por Sun-Tsu,

$$\begin{cases} x \equiv 2 \ (mod\ 3) \\ x \equiv 3 \ (mod\ 5) \\ x \equiv 2 \ (mod\ 7) \end{cases},$$

temos $c_1 = 2$, $c_2 = 3$, $c_3 = 2$, $t_1 = 35$, $t_2 = 21$ e $t_3 = 15$. Agora resolvemos as congruências $35y \equiv 1 \ (mod\ 3)$, $21y \equiv 1 \ (mod\ 5)$ e $15y \equiv 1 \ (mod\ 7)$ obtendo $y_1 = 2$, $y_2 = 1$, $y_3 = 1$ e $x = 233 \equiv 23 \ (mod\ 105)$. Logo, $\{23 + 105k; k \in \mathbb{Z}\}$ é o conjunto solução e 23 é a menor solução positiva.

Por outro lado, para o sistema estudado por Brahmagupta,

$$\begin{cases} x \equiv 2 \ (mod\ 3) \\ x \equiv 3 \ (mod\ 4) \\ x \equiv 4 \ (mod\ 5) \\ x \equiv 5 \ (mod\ 6) \end{cases},$$

não podemos aplicar diretamente o Corolário. Fazemos isso inicialmente para as três primeiras equações, obtendo como solução $x = 59 + 60k$, $k \in \mathbb{Z}$. Desde que $59 + 60k \equiv 5 \ (mod\ 6)$ temos que $\{60k - 1; k \in \mathbb{Z}\}$ é solução e a menor positiva é 59.

1.2 Outras formulações para Teorema Chinês de Restos

Nesta seção trabalharemos apenas com sistemas de congruências cujos coeficientes das variáveis são todos iguais a 1. Os quatro Teoremas desta seção também são chamados de Teorema Chinês de Restos, e podem ser provados usando os Teoremas 1.1.1 e 1.1.2. Entre tais versões do Teorema Chinês de Restos está uma formulação para módulos, e outra para domínios de Dedekind.

Iniciamos com um Lema, que será usado para provar o Teorema Chinês de Restos para sistemas de congruências que envolvem potências de ideais.

Lema 1.2.1 *Sejam $I_1, \cdots, I_n$ ideais do anel A tais que $I_1 + \cdots + I_n = A$. Se $e_1, \cdots, e_n \in \mathbb{N}$ então $I_1^{e_1} + \cdots + I_n^{e_n} = A$.*

Demonstração: Faremos a demonstração por indução sobre n. Quando $n = 2$ temos que $I_1 + I_2 = A$ e existem $x \in I_1$, $y \in I_2$ tais que $1 = x + y$. Segue que $1 = (x+y)^{e_1} = x^{e_1} + \binom{e_1}{1} x^{e_1-1}y + \binom{e_1}{2} x^{e_1-2}y^2 + \cdots + \binom{e_1}{e_1-1} xy^{e_1-1} + y^{e_1}$. Mas, $x = 1 - y$, e então $1 = x^{e_1} + \alpha$, onde α é um somatório de parcelas multiplicadas por $y \in I_2$.

Logo, $1 \in I_1^{e_1} + I_2$, ou seja, $I_1^{e_1} + I_2 = A$. Sendo assim, existem $a \in I_1^{e_1}$ e $b \in I_2$ tais que $1 = a+b$. Então, $1 = (a+b)^{e_2} = a^{e_2} + \binom{e_2}{1} a^{e_2-1}b + \cdots + \binom{e_2}{e_2-1} ab^{e_2-1} + b^{e_2}$. Como $b = 1-a$, então $1 = b^{e_2} + \beta$, onde β é um somatório de parcelas multiplicadas por $a \in I_1^{e_1}$. Segue que $1 \in I_1^{e_1} + I_2^{e_2}$. Logo, $I_1^{e_1} + I_2^{e_2} = A$. Assumimos como hipótese de indução que a afirmação é válida para $n-1$ ideais de A e para quaisquer expoentes naturais. Temos que $A = I_1 + \cdots + I_n = (I_1 + I_2) + I_3 + \cdots + I_n$. Tomando o primeiro expoente igual a 1 e utilizando a hipótese de indução, temos que $A = I_1 + I_2 + I_3^{e_3} + \cdots + I_n^{e_n} = I_1 + (I_2 + I_3^{e_3} + \cdots + I_n^{e_n})$. Pelo caso $n = 2$ e tomando o segundo expoente igual a 1 temos $A = I_1^{e_1} + I_2 + I_3^{e_3} + \cdots + I_n^{e_n} = I_2 + (I_1^{e_1} + I_3^{e_3} + \cdots + I_n^{e_n})$. Novamente pelo caso $n = 2$ e o segundo expoente igual a 1 temos $I_1^{e_1} + I_2^{e_2} + \cdots + I_n^{e_n} = A$.

■

O Lema acima, aplicado sucessivas vezes para $n = 2$, junto com o Teorema 1.1.1 demonstra o próximo Teorema.

Teorema 1.2.1 *Sejam $I_1, \cdots, I_n$ ideais do anel A tais que $I_i + I_j = A$ para $i \neq j$. Para quaisquer $a_1, \cdots, a_n \in A$ e $e_1, \cdots, e_n \in \mathbb{N}$, o sistema*

$$\begin{cases} x \equiv a_1 \ (mod\ I_1^{e_1}) \\ \quad \vdots \\ x \equiv a_n \ (mod\ I_n^{e_n}) \end{cases},$$

tem solução única módulo $I_1^{e_1} \cdots I_n^{e_n}$.

Veremos no capítulo seguinte que este resultado aplicado ao anel $\mathbb{Z}$ e a ideais primos distintos é equivalente ao Teorema da Aproximação para os valores absolutos p-ádicos de $\mathbb{Q}$.

Existe uma versão do Teorema Chinês de Restos que é freqüentemente usada em Álgebra Comutativa. Para apresentá-la, tomamos $I_1, \cdots, I_n$ ideais do anel A e

consideramos o anel $R = \frac{A}{I_1} \times \cdots \times \frac{A}{I_n}$ com as operações usuais, isto é, componente a componente. Claramente a aplicação

$$\varphi : A \to R$$

$$a \mapsto (a + I_1, \cdots, a + I_n)$$

é um homomorfismo de anéis com Kernel $I_1 \cap \cdots \cap I_n$. Pelo Primeiro Teorema do Homomorfismo,

$$\overline{\varphi} : \frac{A}{I_1 \cap \cdots \cap I_n} \to R$$

$$\overline{a} \mapsto \varphi(a)$$

é um monomorfismo. Note que $\overline{\varphi}$ é sobrejetora exatamente quando φ for sobrejetora. Além disso, $\overline{\varphi}$ sobrejetora se e somente se, dados $a_1, \cdots, a_n \in A$ existe $x \in A$ tal que $\overline{\varphi}(\overline{x}) = \varphi(x) = (x + I_1, \cdots, x + I_n) = (a_1 + I_1, \cdots, a_n + I_n)$. Assim, $\overline{\varphi}$ é um isomorfismo se e somente se, o sistema

$$\begin{cases} x \equiv a_1 \ (mod\ I_1) \\ \quad \vdots \\ x \equiv a_n \ (mod\ I_n) \end{cases},$$

tem solução.

O desenvolvimento acima, junto com o Lema 1.1.2 e o Teorema 1.1.2 prova o seguinte Teorema.

Teorema 1.2.2 *Sejam $I_1, \cdots, I_n$ ideais do anel A. São equivalentes:*

(i) $I_1, \cdots, I_n$ são comaximais dois a dois;

(ii) Para quaisquer $a_1, \cdots, a_n \in A$, o sistema

$$\begin{cases} x \equiv a_1 \ (mod\ I_1) \\ \quad \vdots \\ x \equiv a_n \ (mod\ I_n) \end{cases},$$

tem solução;

(*iii*) *O homomorfismo* $\varphi : A \to \frac{A}{I_1} \times \cdots \times \frac{A}{I_n}$, *dado por* $\varphi(a) = (a + I_1, \cdots, a + I_n)$, *é sobrejetor;*

(*iv*) *O homomorfismo* $\overline{\varphi} : \frac{A}{I_1 \cap \cdots \cap I_n} \to \frac{A}{I_1} \times \cdots \times \frac{A}{I_n}$, *dado por* $\overline{\varphi}(\overline{a}) = (a + I_1, \cdots, a + I_n)$, *é um isomorfismo.*

Além disso, $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$.

No Teorema anterior, fazendo $A = \mathbb{Z}$ e $I_i = < m_i >$, com $m_i \in \mathbb{Z}$ e $mdc(m_i, m_j) = 1$ para $i \neq j$, obtemos o isomorfismo clássico entre $\mathbb{Z}_{m_1 \cdots m_n}$ e $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$. Mais ainda, combinando o Teorema acima com o Teorema 1.2.1, vemos que se $m \in \mathbb{N}$ tem decomposição em primos distintos dada por $m = p_1^{e_1} \cdots p_t^{e_t}$, $e_i \in \mathbb{N}$, então $\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_t^{e_t}}$.

Um Teorema Chinês de Restos para módulos pode ser obtido a partir do Teorema 1.2.2. Para isso, lembramos que se M é um A-módulo e I é um ideal de A então o conjunto

$$M \cdot I = \{\sum_{i=1}^{n} m_i u_i; n \in \mathbb{N}, m_i \in M \text{ e } u_i \in I\}$$

é um submódulo de M. Assim podemos considerar o A-módulo $\frac{M}{M \cdot I}$.

Teorema 1.2.3 *Sejam* $I_1, \cdots, I_n$ *ideais de* A, *dois a dois comaximais, e* M *um* $A-$*módulo.*

(*a*) *Dados* $m_1, \cdots, m_n \in M$ *o sistema*

$$\begin{cases} x \equiv m_1 \ (mod\ MI_1) \\ \quad \vdots \\ x \equiv m_n \ (mod\ MI_n) \end{cases},$$

tem solução em M;

(*b*) *A aplicação* $f : \frac{M}{\bigcap_{i=1}^{n} MI_i} \to \frac{M}{MI_1} \times \cdots \times \frac{M}{MI_n}$, *dada por* $f(\overline{m}) = (m+I_1, \cdots, m+I_n)$ *é um isomorfismo de A-módulos.*

Demonstração:

(*a*) Desde que os ideais são dois a dois comaximais temos $I_i + \bigcap_{\substack{j=1 \\ j\neq i}}^{n} I_j = A$. Assim, chamando $J_i = \bigcap_{\substack{j=1 \\ j\neq i}}^{n} I_j$ e usando o Teorema 1.2.2, vem que para cada $i \in \{1, \cdots, n\}$ o sistema

$$\begin{cases} x \equiv 1 \ (mod \ I_i) \\ x \equiv 0 \ (mod \ J_i) \end{cases},$$

tem solução $z_i \in A$. Logo, $z_i - 1 \in I_i$ e $z_i \in I_j$ para todo $j \neq i$. Tomando

$$z = m_1 z_1 + \cdots + m_n z_n \in M$$

temos que $z - m_i = m_i(z_i - 1) + \sum_{\substack{j=1 \\ j\neq i}}^{n} m_j z_j \in MI_i$. Portanto, z é a solução procurada.

(*b*) É claro que f é um monomorfismo de A-módulos. A sobrejetividade segue do item (*a*).

■

Nosso próximo objetivo é apresentar uma formulação do Teorema Chinês de Restos para Domínios de Dedekind.

Em Teoria de Números Algébricos prova-se que todo ideal não nulo, do anel de inteiros algébricos de um corpo de números algébricos, possui fatoração única como produto de potências de ideais primos. Noether provou que esta e outras propriedades do anel de inteiros, podem ser estendidas para uma classe maior de domínios, chamados domínios de Dedekind. As demonstrações das afirmações acima podem ser vistas em ([6], Corolário 8.2, p. 70) e ([6], Proposição 8.7, p. 73).

Usando o Teorema Chinês de Restos é possível verificar, por exemplo, que os domínios de Dedekind que têm uma quantidade finita de ideais primos, são domínios

principais, conforme ([6], Teorema 8.17, p. 78).

Definição 1.2.1 *Um domínio D é chamado de domínio de Dedekind quando todo ideal não nulo de D pode ser fatorado de maneira única como produto de potências de ideais primos de D.*

Definição 1.2.2 *Um D-módulo P diz-se projetivo se, dados D-módulos M e N, um homomorfismo sobrejetor $f : M \to N$ e, um homomorfismo $g : P \to N$, sempre existe um homomorfismo $\overline{g} : P \to M$ tal que $f \circ \overline{g} = g$.*

Uma caracterização útil dos domínios de Dedekind é a seguinte:

Proposição 1.2.1 *Seja D um domínio. São equivalentes:*

(i) *D é um domínio de Dedekind;*

(ii) *D é um anel hereditário, isto é, todo ideal de D é um D-módulo projetivo;*

(iii) *D é integralmente fechado, isto é, D é integral sobre seu corpo de frações;*
D é noetheriano, ou seja, o conjunto dos seus submódulos, ordenado por inclusão, satisfaz a condição de cadeia ascendente;
Todo ideal primo não nulo de D é um ideal maximal de D.

Demonstração: ([11], Theorem 5.1, pg. 378) e ([21], Proposition 4.1, p.45).

■

Com ajuda da Proposição acima, não é difícil mostrar que todo domínio principal é de Dedekind. Por outro lado, $\mathbb{Q}[X, Y]$ é um domínio fatorial que não é de Dedekind, pois o ideal gerado por X é primo e não é maximal.

Teorema 1.2.4 *Sejam $P_1, \cdots, P_n$ ideais primos não nulos e distintos de um domínio de Dedekind D. Dados $a_1, \cdots, a_n \in D$ e $e_1, \cdots, e_n \in \mathbb{N}$ o sistema*

$$\begin{cases} x \equiv a_1 \ (mod \ P_1^{e_1}) \\ \quad \vdots \\ x \equiv a_n \ (mod \ P_n^{e_n}) \end{cases},$$

tem solução em D.

Demonstração: Pela Proposição 1.2.1 vem que $P_1, \cdots, P_n$ são ideais maximais. Desde que estes ideais são distintos, temos para $i \neq j$ que $P_i \not\subseteq P_j$ e, portanto, $P_i + P_j = A$. Agora o resultado segue do Teorema 1.2.1.

■

Note que a hipótese dos ideais primos serem não nulos é essencial no Teorema acima. Sem esta hipótese, podemos montar em $\mathbb{Z}$ o sistema $\begin{cases} x \equiv 0 \ (mod\ 0) \\ x \equiv 3 \ (mod\ 2) \end{cases}$, que não tem solução em $\mathbb{Z}$.

Existe uma formulação do Teorema Chinês de Restos que está relacionada com a distributividade, da interseção em relação a soma e vice-versa, de ideais de um anel comutativo qualquer. Trataremos disso na seção 1.4.

1.3 Função de Euler

Nesta seção usaremos uma versão do Teorema Chinês de Restos (Teorema 1.2.2), aplicada ao anel $\mathbb{Z}$, para provar uma propriedade bem conhecida da função de Euler. É claro que as propriedades da função de Euler não dependem do Teorema Chinês de Restos, contudo veremos que sua utilização simplifica as demonstrações.

A função de Euler permite-nos calcular o número de geradores do grupo $(\mathbb{Z}_n, +)$, determinar a ordem do grupo multiplicativo dos elementos inversíveis do anel $(\mathbb{Z}_n, +, \cdot)$ e encontrar as raízes n-ésimas primitivas da unidade em um corpo qualquer.

Definição 1.3.1 *A função de Euler é a função* $\Phi : \mathbb{N}^* \to \mathbb{N}^*$ *definida por*

$$\Phi(n) = \#\{m \in \mathbb{N}^*; m \leq n \ e \ mdc(m,n) = 1\}.$$

Segue da definição que $\Phi(1) = 1$ e $\Phi(p) = p - 1$, para cada primo p. Uma conta simples também mostra que se p é primo então $\Phi(p^n) = p^{n-1}.\Phi(p)$. De fato, montando uma seqüência finita com os p^n números $1, 2, \cdots, p^{n-1}, p^n$, vemos que existem exatamente p^{n-1} blocos com p números. Em cada bloco há apenas um número que é múltiplo de p e, portanto, temos p^{n-1} múltiplos de p entre 1 e p^n. Mas são exatamente estes p^{n-1} números que não são primos relativos com p^n. Assim $\Phi(p^n) = p^n - p^{n-1} = p^{n-1}.(p-1) = p^{n-1}\Phi(p)$.

Usaremos o Teorema Chinês de Restos para verificar que se $n = p_1^{e_1} \cdots p_t^{e_t}$ com $p_1 < \cdots < p_t$ primos, então $\Phi(n) = (p_1 - 1)p_1^{e_1-1} \cdots (p_t - 1)p_t^{e_t-1} = n(1 - p_1^{-1}) \cdots (1 - p_t^{-1})$.

Para cada $n \in \mathbb{N}^*$, relacionamos a função de Euler com o número de geradores do grupo $(\mathbb{Z}_n, +)$ e com a ordem do grupo multiplicativo $(U(\mathbb{Z}_n), \cdot)$, formado pelos elementos inversíveis do anel $(\mathbb{Z}_n, +, \cdot)$.

Proposição 1.3.1 *Para $m, n \in N^*$ são equivalentes:*

(i) $\overline{m}$ *gera o grupo* $(\mathbb{Z}_n, +)$;

(ii) $\overline{m}$ *é inversível no anel* $(\mathbb{Z}_n, +, \cdot)$;

(iii) $mdc(m, n) = 1$.

Demonstração:

$(i) \Rightarrow (ii)$ Sabemos que, em particular, $\overline{1} \in \mathbb{Z}_n$. Sendo que $\overline{m}$ gera $(\mathbb{Z}_n, +)$, temos que existe $\overline{x} \in \mathbb{Z}_n$ tal que $\overline{1} = \overline{m} \cdot \overline{x} = \overline{x} \cdot \overline{m}$, donde $\overline{m}$ é inversível.

$(ii) \Rightarrow (iii)$ Sendo $\overline{m}$ inversível em $\mathbb{Z}_n$, temos que existe $\overline{a} \in \mathbb{Z}_n$ tal que $\overline{m} \cdot \overline{a} = \overline{a} \cdot \overline{m} = \overline{1}$, donde $(ma - 1) \in n\mathbb{Z}$, ou ainda, $ma \equiv 1 \pmod{n}$. Então existe $(-b) \in \mathbb{Z}$ tal que $n(-b) = ma - 1$, ou seja, $1 = ma + nb$. Pela Identidade de Bezout, segue que $mdc(m, n) = 1$.

$(iii) \Rightarrow (i)$ Segue da hipótese que existem $a, b \in \mathbb{Z}$ tais que $am + bn = 1$, ou ainda $\overline{am} + \overline{bn} = \overline{1}$. Dado $\overline{x} \in \mathbb{Z}_n$, temos que $\overline{x} = \overline{x} \cdot \overline{1} = \overline{x} \cdot (\overline{am} + \overline{bn}) = \overline{max} + \overline{0} = \overline{m} \cdot \overline{ax}$.

Portanto, $\overline{m}$ gera $(\mathbb{Z}_n, +)$.

■

Observe que podemos concluir da Proposição anterior que:

(1) $\Phi(n) = \mid U(\mathbb{Z}_n) \mid$;

(2) $(\mathbb{Z}_n, +, \cdot)$ é corpo se e somente se n é primo.

Proposição 1.3.2 *Se $m, n \in N^*$ e $mdc(m,n) = 1$ então $\Phi(m \cdot n) = \Phi(m) \cdot \Phi(n)$.*

Demonstração: Desde que m e n são primos relativos, os ideais $< m > = m\mathbb{Z}$ e $< n > = n\mathbb{Z}$ são comaximais. Pelo Teorema 1.2.2 vem que $\mathbb{Z}_{m \cdot n}$ e $\mathbb{Z}_m \times \mathbb{Z}_n$ são isomorfos. Logo, têm o mesmo número de elementos inversíveis. Além disso, é fácil ver que $U(\mathbb{Z}_m \times \mathbb{Z}_n) = U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$ e, pela Proposição 1.3.1, temos $\Phi(mn) = \mid U(\mathbb{Z}_{mn}) \mid = \mid U(\mathbb{Z}_m \times \mathbb{Z}_n) \mid = \mid U(\mathbb{Z}_m) \mid \cdot \mid U(\mathbb{Z}_n) \mid = \Phi(m) \cdot \Phi(n)$.

■

Corolário 1.3.1 *Se $n \in \mathbb{N}^*$ e $n = p_1^{e_1} \cdots p_t^{e_t}$, onde $p_1, \cdots, p_t$ são primos distintos então $\Phi(n) = (p_1 - 1)p_1^{e_1 - 1} \cdots (p_t - 1)p_t^{e_t - 1} = n(1 - p_1^{-1}) \cdots (1 - p_t^{-1})$.*

Demonstração: Segue do fato de $p_1, \cdots, p_t$ serem primos distintos, que $mdc(p_i, p_j) = 1$ para $i \neq j$, $i, j \in \{1, \cdots, t\}$. Além disto, podemos afirmar que $mdc(p_i^{e_i}, p_j^{e_j}) = 1$, quando $i \neq j$ e $i, j \in \{1, \cdots, t\}$, e $mdc(p_i^{e_i}, p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} \cdot p_{i+1}^{e_{i+1}} \cdots p_t^{e_t}) = 1$. Assim, $\Phi(p_i^{e_i} \cdot (p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} \cdot p_{i+1}^{e_{i+1}} \cdots p_t^{e_t})) = \Phi(p_i^{e_i}) \cdot \Phi(p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} \cdot p_{i+1}^{e_{i+1}} \cdots p_t^{e_t})$, donde $\Phi(n) = \Phi(p_1^{e_1}) \cdots \Phi(p_t^{e_t})$. Segue que $\Phi(n) = p_1^{e_1 - 1}\Phi(p_1) \cdots p_t^{e_t - 1}\Phi(p_t) = \frac{p_1^{e_1}}{p_1}\Phi(p_1) \cdots \frac{p_t^{e_t}}{p_t}\Phi(p_t) = n \cdot p_1^{-1}(p_1 - 1) \cdot p_2^{-1}(p_2 - 1) \cdots p_t^{-1}(p_t - 1) = n \cdot (1 - p_1^{-1}) \cdot (1 - p_2^{-1}) \cdots (1 - p_t^{-1})$.

■

O Corolário acima mostra que é fácil contar o número de geradores do grupo $(\mathbb{Z}_n, +)$, bem como determinar a ordem do grupo multiplicativo dos elementos inversíveis do anel $(\mathbb{Z}_n, +, \cdot)$. Um raciocínio análogo mostra que também é fácil contar e encontrar as raízes n-ésimas primitivas da unidade em um corpo qualquer.

Definição 1.3.2 *Sejam $\mathbb{K}$ um corpo, $u \in \mathbb{K}$ e $n \in \mathbb{N}^*$. Dizemos que u é uma raiz n-ésima da unidade quando $u^n = 1$. Se além disso, $u^m \neq 1$ para todo $m < n$, $m \in \mathbb{N}^*$, então u é uma raiz n-ésima primitiva da unidade.*

Exemplo

Em $\mathbb{Z}_3$ temos que $\overline{2}$ é raiz quarta da unidade, mas não é raiz quarta primitiva. No entanto $\overline{2}$ é raiz segunda primitiva da unidade.

Considerando u como elemento do grupo multiplicativo $\mathbb{K}^*$ e denotando a ordem dele por $\theta(u)$ vemos que:

- u é raiz n-ésima da unidade quando $\theta(u) \mid n$;
- u é raiz n-ésima primitiva da unidade quando $\theta(u) = n$.

Denotamos por $W_n(\mathbb{K})$ o conjunto das raízes n-ésimas da unidade em $\mathbb{K}$, isto é,

$$W_n(\mathbb{K}) = \{u \in \mathbb{K}; u^n = 1\}.$$

Note que $W_n(\mathbb{K})$ é subgrupo de $(\mathbb{K}^*, \cdot)$. De fato $1 \in W_n(\mathbb{K})$ e, dados $a, b \in W_n(\mathbb{K})$, temos que $a^n = 1$ e $b^n = 1$, donde $(ab)^n = a^n \cdot b^n = 1$, ou seja, $ab \in W_n(\mathbb{K})$; e $(a^{-1})^n = a^{-n} = (a^n)^{-1} = 1^{-1} = 1$, donde $a^{-1} \in W_n(\mathbb{K})$.

Como os elementos de $W_n(\mathbb{K})$ são raízes de $X^n - 1 \in \mathbb{K}[X]$, vemos que $\mid W_n(\mathbb{K}) \mid \leq n$. Quando $\mathbb{K}$ é algebricamente fechado então $\mid W_n(\mathbb{K}) \mid = n$ para todo $n \in \mathbb{N}^*$, em particular $\mid W_n(\mathbb{C}) \mid = n$. Se $\mathbb{K} \subseteq \mathbb{R}$ então $W_n(\mathbb{K}) = \{1\}$ se n é ímpar e $W_n(\mathbb{K}) = \{\pm 1\}$ se n é par.

Se $\mathbb{K}$ possui uma raiz n-ésima primitiva da unidade u então $W_n(\mathbb{K})$ é um grupo cíclico de ordem n, pois $\theta(u) = n$. Neste caso sabemos que $(W_n(\mathbb{K}), \cdot)$ é isomorfo a $(\mathbb{Z}_n, +)$. Este isomorfismo pode ser explicitado por

$$u : (\mathbb{Z}_n, +) \to (W_n(\mathbb{K}), \cdot)$$
$$\overline{m} \mapsto u^m.$$

Assim, os grupos $(\mathbb{Z}_n, +)$ e $(W_n(\mathbb{K}), \cdot)$ têm o mesmo número de geradores, a saber $\Phi(n)$. Desde que os geradores de $W_n(\mathbb{K})$ são elementos de ordem n, eles são exatamente as raízes n-ésimas primitivas da unidade. De outra forma: $(W_n(\mathbb{K}), \cdot)$ tem $\Phi(n)$ raízes n-ésimas primitivas da unidade.

1.4 Aritmética de Ideais

Como citamos na seção 1.2, existe uma versão do Teorema Chinês de Restos relacionada com a distributividade, da soma em relação à interseção e vice-versa, de ideais de uma anel comutativo qualquer. A presente seção tem por objetivo estudar esta relação bem como mostrar que um anel satisfaz o Teorema Chinês de Restos se e somente se tal anel é aritmético.

Dados I, J e J' ideais do anel A, as propriedades abaixo podem ser facilmente verificadas:

(d_1) $I \cdot (J + J') = (I \cdot J) + (I \cdot J')$;

(d_2) $(I \cap J) \cdot (I + J) \subseteq (I \cdot J)$;

(d_3) $I \cdot (J \cap J') \subseteq (I \cdot J) \cap (I \cdot J')$;

(d_4) $(I \cap J) + (I \cap J') \subseteq I \cap (J + J')$;

(d_5) $I + (J \cap J') \subseteq (I + J) \cap (I + J')$.

Quando existe uma relação de inclusão entre I, J, e J', claramente temos:

- $I + (J \cap J') = (I + J) \cap (I + J')$;
- $I \cap (J + J') = (I \cap J) + (I \cap J')$;
- $I \cdot (J \cap J') = (I \cdot J) \cap (I \cdot J')$;

e quando $I \subseteq J$ ou $J \subseteq I$ também vale

- $(I \cap J) \cdot (I + J) = I \cdot J$.

As inclusões contrárias em (d_2), (d_3), (d_4) e (d_5) estão relacionadas. Seja $\Im$ a família dos ideais de A, e considere as seguintes sentenças:

(d_2) $(I \cap J) \cdot (I + J) = I \cdot J$ para quaisquer $I, J \in \Im$;

(d_3) $I \cdot (J \cap J') = (I \cdot J) \cap (I \cdot J')$ para quaisquer $I, J, J' \in \Im$;

(d_4) $(I \cap J) + (I \cap J') = I \cap (J + J')$ para quaisquer $I, J, J' \in \Im$;

(d_5) $I + (J \cap J') = (I + J) \cap (I + J')$ para quaisquer $I, J, J' \in \Im$.

Proposição 1.4.1 *Com a notação acima temos:*

$$(d_5) \Leftrightarrow (d_4) \Rightarrow (d_3) \Rightarrow (d_2).$$

Demonstração:

$(d_5) \Rightarrow (d_4)$ Por (d_5) temos que $(I \cap J) + (I \cap J') = [(I \cap J) + I] \cap [(I \cap J) + J']$. Desde que $(I \cap J) + I = I$ temos $(I \cap J) + (I \cap J') = I \cap [(I \cap J) + J']$. Novamente por (d_5), temos que $(I \cap J) + (I \cap J') = I \cap [(I + J') \cap (J + J')]$. Desde que $I \cap (I + J') = I$ temos $(I \cap J) + (I \cap J') = I \cap (J + J')$.

$(d_4) \Rightarrow (d_5)$ Por (d_4) temos que $(I+J) \cap (I+J') = [(I+J) \cap I] + [(I+J) \cap J']$. Desde que $(I+J) \cap I = I$ temos $(I+J) \cap (I+J') = I + [(I+J) \cap J']$. Novamente por (d_4), temos que $(I + J) \cap (I + J') = I + [(I \cap J') + (J \cap J')]$. Desde que $I + (I \cap J') = I$ temos $(I + J) \cap (I + J') = I + (J \cap J')$.

$(d_4) \Rightarrow (d_3)$ ([10], exercício 3, item $(b) \Rightarrow (c)$)

$(d_3) \Rightarrow (d_2)$ Para as inclusões abaixo usamos respectivamente: $I, J \subseteq I + J$, que o produto está contido na interseção e, finalmente, (d_3).

$I \cdot J \subseteq [(I + J) \cdot I)] \cdot [(I + J) \cdot J] \subseteq [(I + J) \cdot I] \cap [(I + J) \cdot J] = (I + J) \cdot (I \cap J)$.

■

Para ver que as igualdades em $(d_2), \cdots, (d_5)$ não valem em geral, tomamos $A = \mathbb{K}[X, Y]$, $\mathbb{K}$ corpo, $I = < X >$, $J = < Y >$. Assim $XY \in I \cdot J$, mas $XY \notin (I \cap J) \cdot (I + J)$, isto é, não vale (d_2) e, conseqüentemente, não valem (d_3), (d_4) e (d_5) em geral.

É interessante observar que as sentenças apresentadas em (d_2), (d_3), (d_4) e (d_5) são globais, e as implicações vistas na Proposição 1.4.1 não se generalizam ao caso local, mesmo quando A é domínio. De outra forma: valer (d_i) para ideais específicos não implica necessariamente em valer (d_j), $j \neq i$, para estes mesmos ideais. Ilustramos isso, tomando novamente $A = \mathbb{K}[X, Y]$, $I = < X >$, $J = < Y >$ e $J' = < X, Y >$. Para estes ideais valem as distributividades da interseção em relação à soma, e da soma em relação à interseção, mas $I \cdot J \neq (I \cap J) \cdot (I + J)$ como vimos acima.

Dados $a, b \in A$, usaremos no próximo Teorema a seguinte notação:

$$(a : b) = \{\alpha \in A; a\alpha \in < b >\}.$$

Note que $(a : b)$ é ideal de A.

Lema 1.4.1 *Para um anel A, são equivalentes:*

(*i*) $I \cap (J + J') = (I \cap J) + (I \cap J')$, *para quaisquer* $I, J, J' \in \Im$;

(*ii*) $(a : b) + (b : a) = A$.

Demonstração: [15] ou ([8], p. 23, exercício 8).

■

Teorema 1.4.1 *Se A é um domínio, as sentenças (d_2), (d_3), (d_4) e (d_5) são equivalentes.*

Demonstração: Pela Proposição 1.4.1, basta provar $(d_2) \Rightarrow (d_4)$.

Vamos usar $(ii) \Rightarrow (i)$ do Lema acima. Note que se $a = 0$ então $(a : b) = A$. Portanto podemos assumir que $a \neq 0$. Por (d_2) temos $(< a > + < b >) \cdot (< a > \cap < b >) = < a > \cdot < b >$ e então $ab \in (< a > + < b >) \cdot (< a > \cap < b >)$. Assim, $ab = \sum_{i=1}^{n} (\alpha_i a + \beta_i b) \cdot \gamma_i a$, com $n \in \mathbb{N}$, $\alpha_i, \beta_i, \gamma_i \in A$ e $\gamma_i a = \delta_i b$ para algum $\delta_i \in A$. Distribuindo o produto e agrupando convenientemente $ab = \sum_{i=1}^{n} (\alpha_i \gamma_i a^2 + \beta_i \gamma_i ba) = ua^2 + vab$ para $u = \sum_{i=1}^{n} \alpha_i \gamma_i$, $v = \sum_{i=1}^{n} \beta_i \gamma_i$. Sendo A um domínio e $a \neq 0$, temos $b = ua + vb$, donde $b(1 - v) \in < a >$, ou ainda, $1 - v \in (b : a)$. Por outro lado, $av = \sum_{i=1}^{n} \beta_i (\gamma_i a) = \sum_{i=1}^{n} \beta_i \delta_i b \in < b >$, donde $v \in (a : b)$. Assim, $A = (a : b) + (b : a)$ e vale (d_4).

■

Proposição 1.4.2 *Se A é um domínio principal então as sentenças (d_2), (d_3), (d_4) e (d_5) são verdadeiras.*

Demonstração: Em função da Proposição 1.4.1 basta provar (d_4). Sejam $I = < a >$, $J = < b >$ e $J' = < c >$ ideais de A. Devemos verificar que $< a > \cap (< b > + < c >) \subseteq (< a > \cap < b >) + (< a > \cap < c >)$. Lembre que, dados $x, y \in A$ temos que $< x > + < y >$ é o ideal gerado pelo $mdc(x, y)$, e que $< x > \cap < y >$ é o ideal gerado pelo $mmc(x, y)$. Assim, devemos mostrar que $\alpha \mid \beta$ para

$$\alpha = mdc(mmc(a, b), mmc(a, c)),$$

$$\beta = mmc(a, mdc(b, c)).$$

Consideremos as decomposições em fatores irredutíveis de a, b, c: $a = p_1^{e_1} \cdots p_r^{e_r}$, $b = p_1^{f_1} \cdots p_r^{f_r}$ e $c = p_1^{g_1} \cdots p_r^{g_r}$. Assim, $mdc(b, c) = p_1^{h_1} \cdots p_r^{h_r}$, onde $h_i = min\{f_i, g_i\}$; $\beta = p_1^{\beta_1} \cdots p_r^{\beta_r}$, onde $\beta_i = max\{e_i, h_i\}$; $mmc(a, b) = p_1^{j_1} \cdots p_r^{j_r}$, onde $j_i = max\{e_i, f_i\}$; $mmc(a, c) = p_1^{k_1} \cdots p_r^{k_r}$, onde $k_i = max\{e_i, g_i\}$; $\alpha = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, onde $\alpha_i = min\{j_i, k_i\}$.

Agora basta ver que $\alpha_i \leq \beta_i$, isto é, $min\{max\{e_i, f_i)\}, max\{e_i, g_i)\}\} \leq max\{e_i, min\{f_i, g_i)\}\}$. Isso pode ser visto facilmente separando os seis possíveis casos:

$$e_i \leq f_i \leq g_i,$$

$$e_i \leq g_i \leq f_i,$$

$$f_i \leq e_i \leq g_i,$$

$$f_i \leq g_i \leq e_i,$$

$$g_i \leq e_i \leq f_i,$$

$$g_i \leq f_i \leq e_i.$$

■

Verificaremos a seguir que para $i = 2, \cdots, 5$, a sentença (d_i) pode ser estudada apenas para ideais finitamente gerados. Para isso, chame $\Im^*$ o conjunto dos ideais finitamente gerados de A, e considere as sentenças:

(d_2') $(I \cap J) \cdot (I + J) = I \cdot J$ para quaisquer $I, J \in \Im^*$;

(d_3') $I \cdot (J \cap J') = (I \cdot J) \cap (I \cdot J')$ para quaisquer $I, J, J' \in \Im^*$;

(d_4') $(I \cap J) + (I \cap J') = I \cap (J + J')$ para quaisquer $I, J, J' \in \Im^*$;

(d_5') $I + (J \cap J') = (I + J) \cap (I + J')$ para quaisquer $I, J, J' \in \Im^*$.

Proposição 1.4.3 *Com a notação estabelecida nesta seção temos:*

$$(d_i) \Leftrightarrow (d_i'), \quad i = 2, \cdots, 5.$$

Demonstração: As implicações $(d_i) \Rightarrow (d_i')$ são óbvias. Em virtude de $(d_2), \cdots, (d_5)$, as implicações $(d_i') \Rightarrow (d_i)$ requerem a prova de uma inclusão apenas.

$(d_2') \Rightarrow (d_2)$ Seja $u \in I \cdot J$, então $u = \sum_{i=1}^{n} \alpha_i \beta_i$, $n \in \mathbb{N}$, $\alpha_i \in I$, $\beta_i \in J$. Tomando $I_1 = < \alpha_1, \cdots, \alpha_n >$, $J_1 = < \beta_1, \cdots, \beta_n >$ e usando (d_2') para estes ideais vem que $u \in I_1 \cdot J_1 \subseteq (I_1 \cap J_1) \cdot (I_1 + J_1) \subseteq (I \cap J) \cdot (I + J)$. Portanto, $I \cdot J = (I \cap J) \cdot (I + J)$.

$(d_3') \Rightarrow (d_3)$ Seja $u \in (I \cdot J) \cap (I \cdot J')$, então $u = \sum_{i=1}^{n} \alpha_i \beta_i = \sum_{i=1}^{m} \gamma_i \delta_i$ com $m, n \in \mathbb{N}$, $\alpha_i, \gamma_i \in I$, $\beta_i \in J$ e $\delta_i \in J'$. Tomando $I_1 = < \alpha_1, \cdots, \alpha_n, \gamma_1, \cdots, \gamma_m >$, $J_1 = < \beta_1, \cdots, \beta_n >$, $J_1' = < \delta_1, \cdots, \delta_m >$, e usando (d_3') para estes ideais temos que $u \in (I_1 \cdot J_1) \cap (I_1 \cdot J_1') \subseteq I_1 \cdot (J_1 \cap J_1') \subseteq I \cdot (J \cap J')$. Portanto, $(I \cdot J) \cap (I \cdot J') = I \cdot (J \cap J')$.

$(d_4') \Rightarrow (d_4)$ Seja $u \in I \cap (J + J')$. Então $u = \alpha = \beta + \gamma$, onde $\alpha \in I$, $\beta \in J$ e $\gamma \in J'$. Tomamos $I_1 = < \alpha >$, $J_1 = < \beta >$ e $J_1' = < \gamma >$ e, aplicando (d_4') a estes ideais temos que $u \in I_1 \cap (J_1 + J_1') \subseteq (I_1 \cap J_1) + (I_1 \cap J_1') \subseteq (I \cap J) + (I \cap J)$. Portanto, $(I \cap J) + (I \cap J) = I \cap (J + J')$.

$(d_5') \Rightarrow (d_5)$ Seja $u \in (I + J) \cap (I + J')$. Então $u = \alpha + \beta = \gamma + \delta$, onde $\alpha, \gamma \in I$, $\beta \in J$ e $\delta \in J'$. Sejam $I_1 = < \alpha, \gamma >$, $J_1 = < \beta >$ e $J_1' = < \delta >$. Por (d_5') temos que $u \in (I_1 + J_1) \cap (I_1 + J_1') \subseteq I_1 + (J_1 \cap J_1') \subseteq I + (J \cap J')$. Logo, $(I + J) \cap (I + J') = I + (J \cap J')$.

■

Definição 1.4.1 *Um anel A é aritmético quando vale:*

$$(d_5) : I + (J \cap J') = (I + J) \cap (I + J'), \quad \textit{para quaisquer } I, J, J' \in \Im.$$

Vimos que:

(1) A condição acima precisa ser verificada apenas para ideais finitamente gerados (Proposição 1.4.3);

(2) A é aritmético se e somente se $(I \cap J) + (I \cap J') = I \cap (J + J')$, onde $I, J, J' \in \Im$ (Proposição 1.4.1);

(3) Todo domínio principal é aritmético (Proposição 1.4.2);

(4) Um domínio A é aritmético se e somente se vale uma das condições $(d_2), \cdots, (d_5)$ (Teorema 1.4.1).

Estamos interessados em provar que a condição de um anel ser aritmético é equivalente a uma formulação do Teorema Chinês de Restos. Desta forma não nos aprofundamos em propriedades de tais anéis. Contudo citamos abaixo alguns resultados sobre anéis aritméticos que podem ser encontrados em [8], [10] e [17].

(5) Todo sobreanel de um anel aritmético é um anel aritmético, onde sobreanel é o nome dado à extensão de um anel.

(6) O anel A é aritmético se, e somente se, a inclusão $I \subseteq J$ de ideais de A com J finitamente gerado implica na existência de um ideal J' de A tal que $I = J \cdot J'$.

(7) Num anel aritmético com um número finito de ideais maximais, todo ideal finitamente gerado é principal.

(8) Um anel local, ou seja, um anel que possui um único ideal maximal, é aritmético se, e somente se, seus ideais estão totalmente ordenados por inclusão.

Para um A-módulo M, a distributividade da soma em relação a interseção de submódulos, também define uma classe especial de módulos, chamados módulos distributivos. Assim um anel A é aritmético se e somente se o A-módulo A é distributivo.

Voltemos a falar de sistemas de congruências e do Teorema Chinês de Restos. Lembre que provamos na Proposição 1.1.1, que o sistema

$$\begin{cases} x \equiv a_1 \ (mod \ I_1) \\ x \equiv a_2 \ (mod \ I_2) \end{cases},$$

onde I_1, I_2 são ideais de A e $a_1, a_2 \in A$, tem solução se, e somente se, $a_1 \equiv a_2 \ (mod\ I_1 + I_2)$.

A implicação "somente se" pode ser generalizada para n equações da forma seguinte:

Proposição 1.4.4 *Sejam $I_1, \cdots, I_n$ ideais de A e $a_1, \cdots, a_n \in A$. Se*

$$\begin{cases} x \equiv a_1 \ (mod\ I_1) \\ \quad \vdots \\ x \equiv a_n \ (mod\ I_n) \end{cases},$$

tem solução então $a_i \equiv a_j \ (mod\ I_i + I_j)$.

Demonstração: Imediata.

■

Definição 1.4.2 *Dizemos que um anel A satisfaz o Teorema Chinês de Restos quando vale a recíproca da Proposição 1.4.4.*

Agora relacionamos os anéis aritméticos com a existência de solução para sistema de congruências.

Teorema 1.4.2 *Para um anel A são equivalentes:*

(i) A satisfaz o Teorema Chinês de Restos;

(ii) A é anel aritmético.

Demonstração:

$(i) \Rightarrow (ii)$ Sejam I, J e J' ideais de A. Precisamos verificar apenas que $(I+J)\cap(I+J') \subseteq I+(J\cap J')$. Dado $t \in (I+J)\cap(I+J')$ temos que $t \equiv 0 \ (mod\ I+J)$, $t \equiv 0 \ (mod\ I+J')$ e $t \equiv t \ (mod\ J+J')$. Desde que A satisfaz o Teorema Chinês de

Restos, obtemos uma solução em A para o sistema

$$\begin{cases} x \equiv 0 \ (mod\ I) \\ x \equiv t \ (mod\ J) \\ x \equiv t \ (mod\ J') \end{cases},$$

isto é, existe $x \in A$ tal que $x \in I$ e $x - t \in J \cap J'$. Tomando $-y = x - t$ vem que $t = x + y \in I + (J \cap J')$.

$(ii) \Rightarrow (i)$ Sejam $I_1, \cdots, I_n$ ideais de A e $a_1, \cdots, a_n \in A$ tais que $a_i \equiv a_j \ (mod\ I_i + I_j)$. Vamos mostrar que o sistema

$$\begin{cases} x \equiv a_1 \ (mod\ I_1) \\ \quad \vdots \\ x \equiv a_n \ (mod\ I_n) \end{cases},$$

tem solução por indução sobre n. Quando $n = 2$ temos, pela Proposição 1.1.1, que o sistema tem solução. Como hipótese de indução temos que existe $y \in A$ tal que y é solução do sistema

$$\begin{cases} x \equiv a_1 \ (mod\ I_1) \\ \quad \vdots \\ x \equiv a_{n-1} \ (mod\ I_{n-1}) \end{cases}.$$

Consideremos o seguinte sistema

$$\begin{cases} x \equiv y \ (mod \bigcap_{i=1}^{n-1} I_i) \\ x \equiv a_n \ (mod\ I_n) \end{cases}. \tag{1.3}$$

Como $y - a_n = (y - a_i) + (a_i - a_n) \in I_i + (I_i + I_n) = I_i + I_n$, para todo $i \in \{1, \cdots, n-1\}$, temos que $y \equiv a_n \ (mod \bigcap_{i=1}^{n-1} (I_i + I_n))$. Pela hipótese (ii) temos que $(I_1 + I_n) \cap (I_2 + I_n) \cap \cdots \cap (I_{n-1} + I_n) = (I_1 + \cdots + I_{n-1}) \cap I_n$, isto é, $\bigcap_{i=1}^{n-1} (I_i + I_n) = (\bigcap_{i=1}^{n-1} I_i) + I_n$. Portanto, $y \equiv a_n \ (mod\ (\bigcap_{i=1}^{n-1} I_i) + I_n)$ e, segue da Proposição 1.1.1, que o

sistema (1.3) tem solução $z \in A$. Desde que $z-y \in \bigcap_{i=1}^{n-1} I_i$ temos que $z-y \in I_i$ para $i \in \{1, \cdots, n-1\}$. Além disso, $y - a_i \in I_i$. Logo, $z - a_i \in I_i$, isto é $z \equiv a_i \ (mod\ I_i)$ para todo $i \in \{1, \cdots, n-1\}$. Mas z também satisfaz $z \equiv a_n \ (mod\ I_n)$, donde z é solução do sistema.

■

Analisando a demonstração de $(i) \Rightarrow (ii)$ do Teorema 1.4.2 vemos que a hipótese usada foi mais fraca do que a que tínhamos. Usamos apenas o fato de A satisfazer o Teorema Chinês de Restos para três ideais e três elementos quaisquer de A. Isso produz o seguinte Corolário:

Corolário 1.4.1 *Para um anel A são equivalentes:*

(i) *A satisfaz o Teorema Chinês de Restos;*

(ii) *Dados $a_1, a_2, a_3 \in A$ e I_1, I_2, I_3 ideais de A tais que $a_i \equiv a_j \ (mod\ I_i + I_j)$, $i, j \in \{1, 2, 3\}$, o sistema*

$$\begin{cases} x \equiv a_1 \ (mod\ I_1) \\ x \equiv a_2 \ (mod\ I_2) \\ x \equiv a_3 \ (mod\ I_3) \end{cases},$$

tem solução.

Podemos reenunciar o Teorema anterior deixando explícita a parte principal:

Teorema 1.4.3 *Sejam $I_1, \cdots, I_n$ ideais de A. São equivalentes:*

(i) *Para quaisquer $a_1, \cdots, a_n \in A$ tais que $a_i \equiv a_j \ (mod\ I_i + I_j)$ o sistema*

$$\begin{cases} x \equiv a_1 \ (mod\ I_1) \\ \quad \vdots \\ x \equiv a_n \ (mod\ I_n) \end{cases},$$

tem solução em A;

(*ii*) $(I_1 + I_2) \cap (I_1 + I_3) \cap \cdots \cap (I_1 + I_n) \subseteq I_1 + (I_2 \cap I_3 \cap \cdots + I_n)$.

Alguns autores, por exemplo Endler ([6], p. 60), chamam o Teorema 1.4.3 de Teorema Chinês de Restos. Preferimos chamar, neste trabalho, de Teorema Chinês de Restos o Teorema 1.1.1, pois a partir dele provamos formulações para o Teorema Chinês de Restos que aparecem em várias situações, com vimos nas seções 1.1 e 1.2.

Claramente os Teoremas 1.1.1 e 1.4.3 não são equivalentes. O Teorema 1.1.1 tem a vantagem de garantir solução para sistemas de congruências mais gerais, já que admite coeficientes quaisquer para as variáveis. No entanto, quando todos estes coeficientes são iguais a 1, a comaximalidade dos ideais implica na condição $a_i \equiv a_j \ (mod\ I_i + I_j)$, e então, pelo Teorema 1.4.3, temos a distributividade da soma em relação a interseção.

Capítulo 2

Valores Absolutos e Teorema da Aproximação

No capítulo anterior falamos sobre o Teorema Chinês de Restos. Sendo que não faz sentido falarmos sobre tal Teorema para corpos, iremos substitui-lo pelo Teorema da Aproximação para valores absolutos. Assim, inicialmente, definiremos tais valores bem como mostraremos alguns resultados que envolvam tal conceito. Além disto, uma versão mais forte do Teorema da Aproximação nos permite encontrar ordens para um corpo.

Alguns conceitos e alguns resultados a respeito de topologia permitem-nos demonstrar uma versão topológica do Teorema da Aproximação para corpos topológicos e, além disto, mostrar que valores absolutos equivalentes geram topologias equivalentes e vice-versa.

Os valores absolutos não-arquimedianos permitem-nos definir as valorizações exponenciais e, através delas, obtemos uma nova versão do Teorema da Aproximação.

2.1 Valores Absolutos

Esta primeira seção tem por objetivo a definição de valor absoluto bem como falar de algumas suas propriedades. Os valores absolutos são definidos para um corpo $\mathbb{K}$, mas veremos que o corpo de frações de um domínio fatorial permite-nos definir os valores absolutos p-ádicos. Trataremos também dos valores absolutos equivalentes, arquimedianos e não-arquimedianos e veremos que, dados dois valores absolutos equivalentes, temos que um deles é arquimediano se e somente se o outro também o for.

Em toda esta seção denotaremos por $\mathbb{K}$ um corpo qualquer.

Definição 2.1.1 *Dizemos que a função $\varphi : \mathbb{K} \to \mathbb{R}_+$ é um valor absoluto de $\mathbb{K}$ se as seguintes condições são satisfeitas:*

(VA_1) $\varphi(x) = 0$ *se, e somente se,* $x = 0$;

(VA_2) $\varphi(xy) = \varphi(x).\varphi(y)$, *para todos* $x, y \in \mathbb{K}$;

(VA_3) $\varphi(x + y) \leq \varphi(x) + \varphi(y)$, *para todos* $x, y \in \mathbb{K}$.

As condições (VA_1) e (VA_2) expressam que a função φ é um homomorfismo entre os grupos abelianos $(\mathbb{K}^*, .)$ e $(\mathbb{R}_+^*, .)$. A condição (VA_3) é chamada de desigualdade triangular.

Exemplos:

1. Valor absoluto usual: O Exemplo mais conhecido de valor absoluto é o valor absoluto usual de $\mathbb{C}$, com suas restrições aos subcorpos de $\mathbb{C}$. Se L é um subcorpo de $\mathbb{C}$ e $z \in L$, o valor absoluto usual é definido pela relação $| z |^2 = z.\overline{z}$, onde $\overline{z}$ indica o conjugado complexo.

2. Valor absoluto trivial: A aplicação $\varphi : \mathbb{K} \to \mathbb{R}^+$ dada por

$$\varphi(x) = \begin{cases} 0, & \text{se} \quad x = 0 \\ 1, & \text{se} \quad x \neq 0 \end{cases}$$

é um valor absoluto de $\mathbb{K}$, chamado de valor absoluto trivial.

3. Valor absoluto p-ádico de $\mathbb{Q}$: Sejam p um número primo fixo e $x \in \mathbb{Q}^*$. Usando o fato de $\mathbb{Z}$ ser um domínio fatorial, podemos escrever de forma única $x = \frac{u}{v}p^n$, onde $n, u, v \in \mathbb{Z}$ e $p \nmid uv$. Definimos a aplicação $\varphi_p : \mathbb{Q} \to \mathbb{R}_+$ por

$$\varphi_p(x) = \begin{cases} 0, & \text{se} \quad x = 0 \\ p^{-n}, & \text{se} \quad x \neq 0 \end{cases}.$$

Vamos verificar que φ_p é um valor absoluto, o qual chamamos de valor absoluto p-ádico de $\mathbb{Q}$. A condição (VA_1) é óbvia e a condição (VA_2) segue da unicidade da decomposição acima. Para verificarmos (VA_3) precisamos trabalhar apenas com o caso $x, y \in \mathbb{Q}\backslash\{0\}$, com $x + y \neq 0$, pois se algum destes elementos for zero a prova é imediata. Assim tomamos $x = \frac{u}{v}p^n$, $y = \frac{r}{s}p^m$ onde $p \nmid uv$ e $p \nmid rs$ e consideramos, sem perda de generalidade, $n \geq m$. Note que esta consideração implica em $\varphi_p(y) = max\{\varphi_p(x), \varphi_p(y)\}$. Assim $x + y = \frac{p^m(sup^{n-m} + vr)}{vs}$ e no caso $n > m$ temos que p não divide o produto $(sup^{n-m} + vr)vs$ já que $p \nmid vs$ e $p \nmid vr$. Segue que para $n > m$ vale $\varphi_p(x+y) = p^{-m} = \varphi_p(y) \leq \varphi_p(x) + \varphi_p(y)$. No caso $m = n$, pode ocorrer que p divida o produto $(sup^{n-m} + vr)vs = (su + vr)vs$. Mas como $p \nmid vs$ devemos ter que $p \mid (su + vr)$ e então $x + y = p^{m'}\frac{\alpha}{vs}$ onde $p \nmid \alpha vs$ e $m' \geq m$. Segue que para $m = n$ vale $\varphi_p(x + y) = p^{-m'} \leq p^{-m} = \varphi_p(y) \leq \varphi_p(x) + \varphi_p(y)$.

No Exemplo acima verificamos que o valor absoluto p-ádico de $\mathbb{Q}$ satisfaz uma condição mais forte que (VA_3), a saber,

(VA_4) $\varphi_p(x + y) \leq max\{\varphi_p(x), \varphi_p(y)\}$ para todos $x, y \in \mathbb{Q}$.

Os valores absolutos que satisfazem (VA_4) são chamados de valores absolutos

não-arquimedianos. Esse assunto será tratado posteriormente.

Os valores absolutos p-ádicos de $\mathbb{Q}$ se destacam pois a partir deles podemos definir o corpo de números p-ádicos, usualmente denotado por $\mathbb{Q}_p$. Resumidamente, podemos dizer que $\mathbb{Q}_p$ é o corpo obtido quando consideramos $\mathbb{Q}$ com o valor absoluto p-ádico e acrescentamos a $\mathbb{Q}$ o limite de todas as seqüências de Cauchy. Esta construção pode ser vista com detalhes em [13].

Observamos que no Exemplo 3 não é essencial trabalhar com o corpo $\mathbb{Q}$, mas sim com o corpo de frações de um domínio fatorial. Também ao definirmos $\varphi_p(\frac{u}{v}p^n) = p^{-n}$ notamos que a base p desta expressão pode ser trocado por uma constante $c \in \mathbb{R}$ tal que $c > 1$. Desta forma, podemos produzir um Exemplo mais geral.

4. Valor absoluto p-ádico: Sejam D um domínio fatorial que não é corpo, $\mathbb{K}$ seu corpo de frações, P o conjunto dos elementos primos não-associados de D e $U(D)$ o conjunto dos elementos inversíveis de D. Dado $x \in \mathbb{K}^*$, usamos o fato de D ser fatorial para escrever de forma única $x = \epsilon \prod_{p \in P} p^{v_p(x)}$ onde $\epsilon \in U(D)$, $v_p(x) \in \mathbb{Z}$ e $v_p(x) \neq 0$ apenas para uma quantidade finita de primos distintos $p \in P$. Note que $P \neq \emptyset$ pois pedimos que D não fosse corpo. Definimos agora, para cada $p \in P$, a aplicação $\varphi_p : \mathbb{K} \to \mathbb{R}_+$ por

$$\varphi_p(x) = \begin{cases} 0, & \text{se } x = 0 \\ c^{-v_p(x)}, & \text{se } x \neq 0 \end{cases}, \quad \text{onde } c \in \mathbb{R} \text{ e } c > 1.$$

Verificaremos que φ_p é um valor absoluto, chamado de valor absoluto p-ádico. Como no Exemplo anterior, a condição (VA_1) é imediata e (VA_2) segue da unicidade da decomposição acima. Para provar a condição (VA_4) tomamos $x, y \in \mathbb{K}$, $x = \epsilon \prod_{p \in P} p^{v_p(x)}$, $y = \epsilon' \prod_{p \in P} p^{v_p(y)}$ e podemos nos restringir apenas ao caso $x, y, x + y \in \mathbb{K}^*$, pois se algum destes elementos for nulo, a demonstração é trivial. Sem perda de generalidade, assumimos que $v_p(y) \leq v_p(x)$. Nesta condição temos

que $\varphi_p(y) \geq \varphi_p(x)$. Agora escrevemos $x = x_1 p^{v_p(x)}$ e $y = y_1 p^{v_p(y)}$, com $x_1, y_1 \in \mathbb{K}^*$ e $v_p(x_1) = v_p(y_1) = 0$. Assim, $x + y = x_1 p^{v_p(x)} + y_1 p^{v_p(y)} = p^{v_p(y)}(x_1 p^{v_p(x)-v_p(y)} + y_1)$ e segue que $v_p(x+y) \geq v_p(y)$. Como $c > 1$, temos que $c^{-v_p(x+y)} \leq c^{-v_p(y)}$ e portanto $\varphi_p(x+y) \leq \varphi_p(y) = max\{\varphi_p(x), \varphi_p(y)\} \leq \varphi_p(x) + \varphi_p(y)$.

No Exemplo anterior, podemos ainda trocar a constante $c > 1$ por uma constante α, com $0 < \alpha < 1$, e então definir para cada primo p a aplicação $\varphi_p : \mathbb{K} \to \mathbb{R}_+$ por

$$\varphi_p(x) = \begin{cases} 0, & \text{se } x = 0, \\ \alpha^{v_p(x)}, & \text{se } x \neq 0 \end{cases},$$

que também é um valor absoluto em $\mathbb{K}$.

Proposição 2.1.1 *Para um valor absoluto φ de $\mathbb{K}$, as seguintes afirmações são verdadeiras:*

(a) *Se $n \in \mathbb{N}$, $x \in \mathbb{K}$ e $x^n = 1$, então $\varphi(x) = 1$;*

(b) $\varphi(-x) = \varphi(x)$, *para todo $x \in \mathbb{K}$;*

(c) $\varphi(x-y) \leq \varphi(x) + \varphi(y)$, *para todos $x, y \in \mathbb{K}$;*

(d) $\varphi(x.y^{-1}) = \varphi(x).[\varphi(y)]^{-1}$, *para todos $x, y \in \mathbb{K}$ com, $y \neq 0$;*

(e) $\mid \varphi(x) - \varphi(y) \mid \leq \varphi(x-y)$, *para todos $x, y \in \mathbb{K}$.*

Demonstração:

(a) Vamos verificar inicialmente que $\varphi(1) = 1$. Por (VA_1) temos que $\varphi(1) \neq 0$ e então existe $z \in \mathbb{R}_+$ tal que $z.\varphi(1) = 1$. Multiplicando a igualdade $\varphi(1) = \varphi(1.1) = \varphi(1).\varphi(1)$ por z vem que $\varphi(1) = 1$. Seja agora $x \in \mathbb{K}$ tal que $x^n = 1$. Por (VA_2) temos que $\varphi(x)^n = \varphi(x^n) = \varphi(1) = 1$, e como $\varphi(x) \in \mathbb{R}_+$, extraímos a raiz n-ésima obtendo $\varphi(x) = 1$.

(b) e (c) Seguem diretamente da definição e do item (a).

(*d*) Como $y \neq 0$, existe $y^{-1} \in \mathbb{K}$ tal que $y.y^{-1} = 1$. Por (VA_2) e pelo item (a) temos que $\varphi(y^{-1}) = [\varphi(y)]^{-1}$. Então, $\varphi(x.y^{-1}) = \varphi(x).\varphi(y^{-1}) = \varphi(x).[\varphi(y)]^{-1}$.

(*e*) Sabemos que $\varphi(x) = \varphi(y + (x - y)) \leq \varphi(y) + \varphi(x - y)$ e, então $\varphi(x) - \varphi(y) \leq \varphi(x-y)$. Por outro lado, $\varphi(y) = \varphi(x+(y-x)) \leq \varphi(x)+\varphi(y-x) = \varphi(x)+\varphi(x-y)$. Daí, $-\varphi(x-y) \leq \varphi(x)-\varphi(y)$. Logo, $-\varphi(x-y) \leq \varphi(x)-\varphi(y) \leq \varphi(x-y)$, ou seja, $| \varphi(x)-\varphi(y) | \leq \varphi(x-y)$.

■

Um valor absoluto sobre um corpo $\mathbb{K}$, fornece uma forma de comparar elementos de $\mathbb{K}$, através da relação de ordem $\leq$ de $\mathbb{R}_+$. Neste sentido, o valor absoluto trivial não é eficiente. Portanto há interesse em saber quando um corpo possui um valor absoluto não trivial. Esta questão será respondida no próximo Teorema, mas para isso precisamos lembrar algumas definições e apresentar alguns resultados.

Definição 2.1.2 *Dizemos que um anel A tem característica finita se existe um $n \in \mathbb{N}^*$ tal que $n.1 = 0$. Aqui $n.1$ representa a soma da unidade do anel por n vezes. Se A é um anel de característica finita e n é o menor número natural tal que $n.1 = 0$, dizemos que A é um anel de característica n e denotamos isso por $char(A) = n$. Quando A não tem característica finita dizemos que A tem característica zero.*

Exemplo:

$char(\mathbb{C}) = char(\mathbb{R}) = char(\mathbb{Q}) = char(\mathbb{Z}) = char(n\mathbb{Z}) = 0$

$char(\mathbb{Z}_n) = n$

Se D é um domínio, é conhecido que $char(D) = 0$ ou $char(D) = p$, para algum primo positivo p. Sabemos ainda que um corpo de característica 0 contém um subcorpo isomorfo à $\mathbb{Q}$, e um corpo de característica p contém um subcorpo isomorfo à $\mathbb{Z}_p$.

Definição 2.1.3 *Chamamos de corpo primo de um corpo $\mathbb{K}$ ao menor subcorpo contido em $\mathbb{K}$.*

Exemplo:

Se $char(\mathbb{K}) = 0$ então o corpo primo de $\mathbb{K}$ é $\mathbb{Q}$.

Se $char(\mathbb{K}) = p$ então o corpo primo de $\mathbb{K}$ é $\mathbb{Z}_p$.

Lembremos que uma extensão de corpos $\mathbb{K} \subseteq L$ é dita algébrica se todo $\alpha \in L$ é algébrico sobre $\mathbb{K}$, isto é, se para cada $\alpha \in L$ existe $f(X) \in \mathbb{K}[X]$, $f(X) \neq 0$, tal que $f(\alpha) = 0$. Um elemento $\alpha \in L$ que não é algébrico sobre $\mathbb{K}$ é dito transcendente sobre $\mathbb{K}$. Dizemos também que $\mathbb{K} \subseteq L$ é extensão finita se $dim_{\mathbb{K}} L < \infty$, quando vemos L como espaço vetorial sobre $\mathbb{K}$. Usamos as notações $\mathbb{K}[\alpha] = \{f(\alpha); f(X) \in \mathbb{K}[X]\}$, e $\mathbb{K}(\alpha)$ para indicar o menor corpo que contém $\mathbb{K}$ e α.

A Proposição abaixo apresenta resultados conhecidos e sua demonstração pode ser vista em ([12], p. 89 e 90) e ([22], p. 29).

Proposição 2.1.2 *Sejam $\mathbb{K} \subseteq L$ uma extensão de corpos e $\alpha \in L$.*

(a) *Se α é algébrico sobre $\mathbb{K}$ então $\mathbb{K}[\alpha]$ é um subcorpo de L que contém $\mathbb{K}$;*

(b) *Se α é transcendente sobre $\mathbb{K}$ então $\mathbb{K}[\alpha]$ é um subdomínio de L que contém $\mathbb{K}$ e $\mathbb{K}[\alpha]$ não é corpo;*

(c) *Se α é algébrico sobre $\mathbb{K}$ e $\mathbb{K} = \mathbb{Z}_p$ então $\mathbb{K}[\alpha]$ é um corpo com p^n elementos;*

(d) *Se $\mathbb{K} \subseteq L$ é extensão finita então $\mathbb{K} \subseteq L$ é extensão algébrica.*

(e) *Se $\mathbb{K} \subseteq L$ e $L \subseteq F$ são extensões algébricas, então $\mathbb{K} \subseteq F$ é extensão algébrica.*

Para caracterizar os corpos que possuem valor absoluto não-trivial, usaremos também o seguinte Lema:

Lema 2.1.1 *Seja $\mathbb{K} \subseteq L$ uma extensão de corpos e φ um valor absoluto de $\mathbb{K}$. Se $\mathbb{K} \subseteq L$ é extensão algébrica então φ pode ser estendida a um valor absoluto $\overline{\varphi}$ sobre L.*

Demonstração: ([24], p. 63)

Teorema 2.1.1 *As seguintes condições são equivalentes:*

(i) $\mathbb{K}$ *admite valor absoluto não-trivial;*

(ii) $\mathbb{K}$ *não é extensão algébrica de um corpo finito.*

Demonstração:

$(i) \Rightarrow (ii)$ Seja φ um valor absoluto sobre $\mathbb{K}$ e suponha que $\mathbb{K}$ é extensão algébrica de um corpo finito F. Então F tem característica p e $\mathbb{Z}_p \subseteq F$, implicando em $dim_{\mathbb{Z}_p} F < \infty$, pois F é finito. Segue da Proposição 2.1.2, item (d), que $\mathbb{Z}_p \subseteq F$ é extensão algébrica e portanto $\mathbb{Z}_p \subseteq \mathbb{K}$ é extensão algébrica, pelo item (e) da Proposição 2.1.2. Dado $\alpha \in \mathbb{K}^*$ temos que α é algébrico sobre $\mathbb{Z}_p$, e novamente pela Proposição 2.1.2, $\mathbb{Z}_p[\alpha]$ é um corpo com p^n elementos. Como $(\mathbb{Z}_p[\alpha]^*, .)$ é um grupo com $p^n - 1$ elementos e $\alpha \in \mathbb{Z}_p[\alpha]^*$, vem que $\alpha^{p^n-1} = 1$. Assim $\varphi(\alpha^{p^n-1}) = [\varphi(\alpha)]^{p^n-1} = 1$ que garante que $\varphi(\alpha) = 1$. Portanto, se $\mathbb{K}$ admite valor absoluto não-trivial então $\mathbb{K}$ não é extensão algébrica de um corpo finito.

$(ii) \Rightarrow (i)$ Seja $\mathbb{K}_0$ o corpo primo de $\mathbb{K}$. Consideremos inicialmente que $\mathbb{K}$ seja uma extensão algébrica de $\mathbb{K}_0$. Neste caso nossa hipótese não permite que $\mathbb{K}_0$ seja da forma $\mathbb{Z}_p$, e então $\mathbb{K}_0 = \mathbb{Q}$. Assim $\mathbb{K}$ é uma extensão algébrica de $\mathbb{Q}$ e, portanto, $\mathbb{K} \subseteq \mathbb{C}$, e temos um valor absoluto não-trivial em $\mathbb{K}$ obtido pela restrição do valor absoluto usual de $\mathbb{C}$. Consideremos agora o caso onde $\mathbb{K}$ não é extensão algébrica de $\mathbb{K}_0$. Seja β uma base do subespaço que contém todos os elementos transcendentes. Então $\beta \neq \emptyset$ e fixamos $b \in \beta$. Tomamos L como sendo o menor corpo que contém K_0 e $\beta - \{b\}$, isto é, $L = \mathbb{K}_0(\beta - \{b\})$. É claro que $\mathbb{K}_0 \subseteq L \subseteq L[b] \subseteq \mathbb{K}$ e que $\mathbb{K}$ é uma extensão algébrica de $L[b]$, pois todo elemento de $\mathbb{K}$ que não é algébrico sobre $\mathbb{K}_0$ já está em $L[b]$. Notemos ainda que $L[b]$ é um domínio que não é corpo, pois b não é algébrico sobre L, por construção. Usando o Exemplo 4, podemos construir uma valor absoluto p-ádico no corpo de frações de $L[b]$, mas em particular, podemos

tomar este valor absoluto p-ádico, que não é trivial, em $L[b]$. Finalmente, concluímos que existe um valor absoluto não-trivial em $\mathbb{K}$, pelo Lema 2.2.1, já que $\mathbb{K}$ é extensão algébrica de $L[b]$.

■

Corolário 2.1.1 *Se $\mathbb{K}$ é finito então $\mathbb{K}$ admite apenas o valor absoluto trivial.*

Demonstração: A demonstração segue imediatamente do Teorema 2.1.1.

■

Nosso próximo objetivo é mostrar o Teorema da Aproximação para valores absolutos. Sendo que o enunciado de tal Teorema envolve valores absolutos não-equivalentes, falaremos sobre estes, bem como sobre valores absolutos equivalentes e algumas de suas propriedades.

Definição 2.1.4 *Sejam φ, ψ dois valores absolutos de $\mathbb{K}$. Dizemos que φ e ψ são equivalentes se existe um número real $\rho > 0$ tal que $\varphi = \psi^\rho$.*

Exemplos:

1. Dado $x = a + ib \in \mathbb{C}$, definimos:

- $| x |_1 = a^2 + b^2$
- $| x |_2 = (a^2 + b^2)^{\frac{1}{2}}$

É fácil ver que $| \cdot |_1$ e $| \cdot |_2$ são valores absolutos de $\mathbb{C}$, e como $| \cdot |_1 = (| \cdot |_2)^2$ temos que estes valores absolutos são equivalentes.

2. Se p e q são primos distintos em $\mathbb{Z}$, então os valores absolutos p-ádico e q-ádico não são equivalentes. De fato, dados p e q primos distintos temos que $\varphi_p(p) = p^{-1} = \frac{1}{p}$ e $\varphi_q(p) = p^0 = 1$. Supomos que φ_p e φ_q são equivalentes, ou seja, existe $\rho > 0$, $\rho \in \mathbb{R}$, tal que $(\varphi_p)^\rho = \varphi_q$. Então, $(\frac{1}{p})^\rho = [\varphi_p(p)]^\rho = \varphi_q(p) = 1$. Usando as propriedades logarítmicas, temos que $\rho = 0$, o que é absurdo, donde φ_p e φ_q não são equivalentes.

Proposição 2.1.3 *O valor absoluto trivial de $\mathbb{K}$ é equivalente apenas a si mesmo.*

Demonstração: Sejam φ o valor absoluto trivial de $\mathbb{K}$ e ψ um valor absoluto equivalente a φ. Então existe $\rho > 0$, $(\rho \in \mathbb{R})$ tal que $\varphi = \psi^\rho$. Para $x \in \mathbb{K}$, $x \neq 0$, temos $[\psi(x)]^\rho = \varphi(x) = 1$ e então $\rho\, ln[\psi(x)] = 0$ o que implica em $\psi(x) = 1$. Logo, ψ é o valor absoluto trivial.

■

Um resultado provado por Ostrowski em 1935, garante que os únicos valores absolutos de uma extensão finita de $\mathbb{Q}$ são, a menos de equivalência, o valor absoluto trivial, a restrição do valor absoluto usual de $\mathbb{C}$ e os valores absolutos p-ádicos. A demonstração original está em [20]. O caso particular que mostra este resultado apenas para $\mathbb{Q}$ pode ser visto em [13] ou [7].

Proposição 2.1.4 *Para os valores absolutos não triviais φ, ψ de $\mathbb{K}$, as seguintes afirmações são equivalentes:*

(i) *φ é equivalente à ψ;*

(ii) *Se $x \in \mathbb{K}$ e $\varphi(x) < 1$, então $\psi(x) < 1$;*

(iii) *Para $x \in \mathbb{K}$, $\varphi(x) \leq 1$ se, e somente se, $\psi(x) \leq 1$.*

Demonstração:

(i) $\Rightarrow$ *(ii)* Seja $x \in \mathbb{K}$ tal que $\varphi(x) < 1$. Por hipótese, existe $\rho \in \mathbb{R}$, $\rho > 0$, tal que $\varphi = \psi^\rho$ e então $[\psi(x)]^\rho < 1$, donde $\psi(x) < 1$.

(ii) $\Rightarrow$ *(iii)* Como φ é um valor absoluto não-trivial, existe $y \in \mathbb{K}$, $y \neq 0$, tal que $\varphi(y) \neq 1$. Da igualdade $1 = \varphi(y).\varphi(y^{-1})$, concluímos que $\varphi(y) < 1$ ou $\varphi(y^{-1}) < 1$ e então existe $z \in \mathbb{K}$, $z \neq 0$ $(z = y$ ou $z = y^{-1})$ satisfazendo $0 < \varphi(z) < 1$. Consideramos $x \in \mathbb{K}$ tal que $\varphi(x) \leq 1$. Para todo $n \in \mathbb{N}$, $\varphi(x^n.z) = \varphi(x^n).\varphi(z) = [\varphi(x)]^n.\varphi(z) < 1$ e segue da nossa hipótese *(ii)*, que $\psi(x^n.z) < 1$, ou ainda, $[\psi(x)]^n.\psi(z) < 1$, donde $[\psi(x)]^n < [\psi(z)]^{-1}$ que implica em $\psi(x) \leq 1$. Supomos agora que $\psi(x) \leq 1$. Se $\psi(x) = 0$ então é claro que $x = 0$

e, conseqüentemente, $\varphi(x) \leq 1$. Se $\psi(x) \neq 0$ concluímos que $\psi(x^{-1}) \geq 1$ e, pela contra-positiva do item (ii), temos que $\varphi(x^{-1}) \geq 1$. Segue que $\varphi(x) \leq 1$.

$(iii) \Rightarrow (i)$ Como φ é um valor absoluto não-trivial, as mesmas considerações feitas acima garantem a existência de $z \in \mathbb{K}$, $z \neq 0$, tal que $\varphi(z) > 1$. Aplicando a hipótese (iii), temos que $\psi(z) > 1$. Daí segue que $log(\varphi(z)) > 0$ e $log(\psi(z)) > 0$. Dado $x \in \mathbb{K}$, $x \neq 0$, devemos verificar que $\varphi(x) = (\psi(x))^{\rho}$ para algum $\rho \in \mathbb{R}$, $\rho > 0$. Para isso provaremos antes que $\frac{log(\psi(x))}{log(\psi(z))} = \frac{log(\varphi(x))}{log(\varphi(z))}$. Sejam $m, n \in \mathbb{Z}$ e $n > 0$. Então $\frac{m}{n} \geq \frac{log(\varphi(x))}{log(\varphi(z))}$ se, e somente se, $m\ log(\varphi(z)) \geq n\ log(\varphi(x))$, ou ainda, $log(\varphi(z))^m \geq log(\varphi(x))^n$. Isso é equivalente a dizer que $(\varphi(z))^m \geq (\varphi(x))^n$. Tal desigualdade é verdadeira se, e somente se, $\frac{\varphi(x^n)}{\varphi(z^m)} \leq 1$, ou ainda $\varphi(x^n.z^{-m}) \leq 1$. Por hipótese, $\varphi(x^n.z^{-m}) \leq 1$ se, e somente se, $\psi(x^n.z^{-m}) \leq 1$, isto é, $(\psi(x))^n \leq (\psi(z))^m$. Mas $(\psi(x))^n \leq (\psi(z))^m$ se, e somente se, $log(\psi(x))^n \leq log(\psi(z))^m$, ou ainda, $n\ log(\psi(x)) \leq m\ log(\psi(z))$ o qual vale se, e somente se, $\frac{m}{n} \geq \frac{log(\psi(x))}{log(\psi(z))}$ para todo $x \in \mathbb{K}\backslash\{0\}$. Portanto $\frac{m}{n} \geq \frac{log(\varphi(x))}{log(\varphi(z))}$ se, e somente se, $\frac{m}{n} \geq \frac{log(\psi(x))}{log(\psi(z))}$. Supomos agora que $\frac{log(\varphi(x))}{log(\varphi(z))} \neq \frac{log(\psi(x))}{log(\psi(z))}$. Sem perda de generalidade podemos considerar $\frac{log(\varphi(x))}{log(\varphi(z))} > \frac{log(\psi(x))}{log(\psi(z))}$ e, pela densidade de $\mathbb{Q}$ em $\mathbb{R}$, existe $\frac{m}{n} \in \mathbb{Q}$, com $n \in \mathbb{Z}_+$ tal que $\frac{log(\varphi(x))}{log(\varphi(z))} > \frac{m}{n} \geq \frac{log(\psi(x))}{log(\psi(z))}$, que implica em $\frac{m}{n} \geq \frac{log(\varphi(x))}{log(\varphi(z))}$, que é uma contradição. Assim, para todo $x \in \mathbb{K}\backslash\{0\}$, $\frac{log(\psi(x))}{log(\psi(z))} = \frac{log(\varphi(x))}{log(\varphi(z))}$. Então $log(\varphi(x)) = log(\psi(x))^{\frac{log(\varphi(z))}{log(\psi(z))}}$. Tomamos $\rho = \frac{log(\varphi(z))}{log(\psi(z))} > 0$. Logo, $log(\varphi(x)) = \rho\ log(\psi(x)) = log(\psi(x))^{\rho}$, donde $\varphi(x) = [\psi(x)]^{\rho}$, para todo $x \in \mathbb{K}$. Portanto, φ é equivalente a ψ.

■

Terminaremos esta seção distinguindo dois tipos de valores absolutos: os arquimedianos e os não-arquimedianos. Vimos nos Exemplos 3 e 4 de valores absolutos que existem valores absolutos que satisfazem uma condição mais forte que a desigualdade triangular, isto é, satisfazem $\varphi(x+y) \leq max\{\varphi(x), \varphi(y)\}$. Nosso interesse em destacar tais valores absolutos ficará claro na última seção deste capítulo, onde veremos que estes valores absolutos estão em correspondência biunívoca com

as valorizações exponenciais. As valorizações exponenciais são casos particulares das valorizações de Krull, que serão estudadas no capítulo 3.

Definição 2.1.5 *Um valor absoluto* $\varphi : \mathbb{K} \to \mathbb{R}_+$ *que satisfaz a condição:*

(VA_4) $\varphi(x+y) \leq max\{\varphi(x), \varphi(y)\}$ *para todos* $x,\ y \in \mathbb{K}$.

é chamado de valor absoluto não-arquimediano. Caso contrário dizemos que o valor absoluto é arquimediano.

Observe que a condição (VA_4) implica na condição (VA_3), pois $\varphi(x+y) \leq max\{\varphi(x), \varphi(y)\} \leq \varphi(x) + \varphi(y)$.

Exemplos:

- O valor absoluto usual de um subcorpo $L \subseteq \mathbb{C}$ é arquimediano pois $1 \in L$ e $\mid 1+1 \mid > max\{\mid 1 \mid, \mid 1 \mid\}$.
- O valor absoluto trivial é não-arquimediano, pois se $max\{\varphi(x), \varphi(y)\} = 0$ temos que $\varphi(x) = \varphi(y) = 0$, donde $x = y = 0$ e $\varphi(x+y) = 0$; por outro lado, se $max\{\varphi(x), \varphi(y)\} = 1$ então $\varphi(x+y) \leq max\{\varphi(x), \varphi(y)\}$, uma vez que φ é trivial.
- Os valores absolutos p-ádicos, de corpos de frações de domínios fatoriais, são não-arquimedianos, como visto no Exemplo 4.

Proposição 2.1.5 *Sejam* φ *um valor absoluto não-arquimediano de* $\mathbb{K}$ *e* $x, y \in \mathbb{K}$. *Se* $\varphi(x) \neq \varphi(y)$ *então* $\varphi(x+y) = max\{\varphi(x), \varphi(y)\}$.

Demonstração: Supomos, sem perda de generalidade, que $max\{\varphi(x), \varphi(y)\} = \varphi(y)$. Então, $\varphi(x+y) \leq max\{\varphi(x), \varphi(y)\} = \varphi(y) = \varphi(x+y-x) \leq max\{\varphi(x+y), \varphi(-x)\} \leq max\{\varphi(x), \varphi(y)\} = \varphi(y)$, ou ainda, $\varphi(y) = max\{\varphi(x+y), \varphi(x)\}$. Supondo que $max\{\varphi(x+y), \varphi(x)\} = \varphi(x)$, teríamos $\varphi(y) = \varphi(x)$, o que é absurdo, pela hipótese. Então $\varphi(y) = \varphi(x+y)$, donde $\varphi(x+y) =$

$max\{\varphi(x), \varphi(y)\}$.

■

O próximo Teorema e seu Corolário apresentam algumas caracterizações para os valores absolutos arquimedianos e não-arquimedianos.

Teorema 2.1.2 *Seja φ um valor absoluto de $\mathbb{K}$. Então são equivalentes:*

(i) φ *é não-arquimediano;*

(ii) Para todo $\rho \in \mathbb{R}_+^*$, φ^ρ *é um valor absoluto não-arquimediano de* $\mathbb{K}$;

(iii) $\varphi(n.1) \leq 1$, $\forall\, n \in \mathbb{N}$;

(iv) $\{\varphi(n.1) : n \in \mathbb{N}\}$ *é limitado;*

(v) Se $\varphi(x) \leq 1$, *então* $\varphi(x+1) \leq 1$, *para todo* $x \in \mathbb{K}$.

Demonstração:

$(i) \Rightarrow (ii)$ É claro que $\varphi^\rho(x) = [\varphi(x)]^\rho = 0$ se, e somente se, $x = 0$ e, $\varphi^\rho(x.y) = [\varphi(x.y)]^\rho = [\varphi(x).\varphi(y)]^\rho = [\varphi(x)]^\rho.[\varphi(y)]^\rho = \varphi^\rho(x).\varphi^\rho(y)$ para todo $x, y \in \mathbb{K}$. Por hipótese φ é um valor absoluto não-arquimediano, logo $\varphi^\rho(x+y) = [\varphi(x+y)]^\rho \leq [max\{\varphi(x), \varphi(y)\}]^\rho = max\{[\varphi(x)]^\rho, [\varphi(y)]^\rho\} = max\{\varphi^\rho(x), \varphi^\rho(y)\}$ para todo $x, y \in \mathbb{K}$. Portanto, φ^ρ é um valor absoluto não-arquimediano de $\mathbb{K}$.

$(ii) \Rightarrow (iii)$ Faremos a demonstração por indução sobre n. Para $n = 1$ é óbvio e vamos assumir como hipótese de indução que $\varphi(n.1) \leq 1$. Por (ii), fazendo $\rho = 1$ temos que φ é não-arquimediano e assim, $\varphi((n+1).1) = \varphi(n.1+1) \leq max\{\varphi(n.1), \varphi(1)\} = 1$. Portanto, $\varphi(n.1) \leq 1$ para todo $n \in \mathbb{N}$.

$(iii) \Rightarrow (iv)$ Imediato.

$(iv) \Rightarrow (v)$ Seja $x \in \mathbb{K}$ tal que $\varphi(x) \leq 1$. Por hipótese, existe $c \in \mathbb{R}$, $c > 0$, tal que $\varphi(n.1) < c$ para todo $n \in \mathbb{N}$. Segue que $[\varphi(x+1)]^n = \varphi((x+1)^n) = \varphi(\sum_{i=0}^{n} \binom{n}{i} x^i) \leq \sum_{i=0}^{n} \varphi(\binom{n}{i} x^i) = \sum_{i=0}^{n} \varphi(\binom{n}{i}.1).\varphi(x^i) \leq \sum_{i=0}^{n} c.[\varphi(x)]^i = c\sum_{i=0}^{n}[\varphi(x)]^i \leq cn + c$, ou seja, $[\varphi(x+1)]^n \leq c.n + c$ para todo $n \in \mathbb{N}$. Daí,

$\varphi(x+1) \leq (cn+c)^{\frac{1}{n}}$. Segue que $\lim_{n\to\infty} \varphi(x+1) \leq \lim_{n\to\infty} (cn+c)^{\frac{1}{n}}$. Logo, $\varphi(x+1) \leq \lim_{n\to\infty} (cn+c)^{\frac{1}{n}}$, donde $log(\varphi(x+1)) \leq log(\lim_{n\to\infty} (cn+c)^{\frac{1}{n}}) = \lim_{n\to\infty} log((cn+c)^{\frac{1}{n}}) = \lim_{n\to\infty} \frac{log(cn+c)}{n} = \lim_{n\to\infty} \frac{\frac{1}{cn+c}\cdot c}{1} = \lim_{n\to\infty} \frac{1}{n+1} = 0$. Portanto, $\varphi(x+1) \leq 1$.

$(v) \Rightarrow (i)$ Sejam $x, y \in \mathbb{K}$. Se um deles, ou ambos, forem iguais a zero, é fácil ver que $\varphi(x+y) = max\{\varphi(x), \varphi(y)\}$. Vamos então analisar o caso em que ambos são diferentes de zero, e assim $\varphi(x), \varphi(y) \neq 0$. Assumimos, sem perda de generalidade, que $\varphi(x) \leq \varphi(y) \neq 0$. Então, $\varphi(\frac{x}{y}) = \varphi(x).\varphi(y^{-1}) = \varphi(x).[\varphi(y)]^{-1} \leq 1$, ou seja, $\varphi(\frac{x}{y}) \leq 1$. Pela hipótese, $\varphi(\frac{x}{y}+1) \leq 1$, e então,

$\varphi(x+y) = \varphi(y(\frac{x}{y}+1)) = \varphi(y).\varphi(\frac{x}{y}+1) \leq \varphi(y).1 = \varphi(y) = max\{\varphi(x), \varphi(y)\}$

Logo, $\varphi(x+y) \leq max\{\varphi(x), \varphi(y)\}$, para todo $x, y \in \mathbb{K}$.

■

O Corolário abaixo dá uma forma simples para verificar quando um valor absoluto é arquimediano.

Corolário 2.1.2 *Seja φ um valor absoluto de $\mathbb{K}$. São equivalentes:*

(i) φ é arquimediano;

(ii) $\varphi(n.1) > 1$, para algum $n \in \mathbb{N}$.

Demonstração: Segue de $(i) \Rightarrow (iii)$ do Teorema acima.

■

Sejam φ e ψ valores absolutos sobre o corpo $\mathbb{K}$ tais que φ é arquimediano e ψ é não-arquimediano. Então φ e ψ não são equivalentes, como conseqüência do seguinte resultado:

Corolário 2.1.3 *Sejam φ e ψ valores absolutos equivalentes de $\mathbb{K}$. Então as seguintes condições são equivalentes:*

(i) φ é não-arquimediano;

(ii) ψ é não-arquimediano.

Demonstração: Como φ e ψ são equivalentes, existe $\rho > 0$, $\rho \in \mathbb{R}$, tal que $\psi = \varphi^\rho$. Assim o resultado segue de $(i) \Leftrightarrow (ii)$ do Teorema.

■

Proposição 2.1.6 *Se $\varphi\,|_{\mathbb{K}_0}$ é trivial para algum subcorpo $\mathbb{K}_0$ de $\mathbb{K}$, então φ é não-arquimediano.*

Demonstração: Assumimos que φ é arquimediano. Então existe $m \in \mathbb{N}$ tal que $\varphi(m.1) > 1$. Como $x = m.1 \in \mathbb{K}_0$, segue que $\varphi\,|_{\mathbb{K}_0}$ é não-trivial.

■

Proposição 2.1.7 *Se $\mathbb{K}$ tem característica não-nula então os valores absolutos de $\mathbb{K}$ são não-arquimedianos.*

Demonstração: Seja p a característica de $\mathbb{K}$. Então existe $K_0 \subseteq K$ tal que K_0 é isomorfo a $\mathbb{Z}_p$. Assim, $(K_0, .)$ é um grupo multiplicativo com $p-1$ elementos, e portanto, dado $0 \neq x \in \mathbb{K}_0$ temos que $x^{p-1} = 1$. Segue que $[\varphi(x)]^{p-1} = 1$, e daí, $\varphi(x) = 1$ para todo $x \in \mathbb{K}_0^*$. Portanto, $\varphi\,|_{\mathbb{K}_0}$ é o valor absoluto trivial, e pela Proposição anterior, φ é não-arquimediano.

■

2.2 Teorema da Aproximação para Valores Absolutos

Nesta seção provaremos o Teorema da Aproximação para Valores Absolutos, que aparece como o substituto em corpos, para o Teorema Chinês de Restos. Mostraremos também uma versão mais forte do Teorema da Aproximação para Valores Absolutos, envolvendo valores absolutos não-arquimedianos, o que possibilita construir ordens para um corpo, sob condições especiais.

O Teorema Chinês de Restos aplicado ao anel $\mathbb{Z}$ e às potências de primos positivos e distintos $p_1^{e_1}, \cdots, p_n^{e_n}$, como enunciado no Teorema 1.2.4 , pode ser formulado através dos valores absolutos p_i-ádicos de $\mathbb{Q}$. De forma mais precisa:

Proposição 2.2.1 *Sejam $p_1, \cdots, p_n$ primos positivos distintos e $a_1, \cdots, a_n \in \mathbb{Z}$. São equivalentes:*

(i) O sistema $x \equiv a_i \ (mod\ p_i^{e_i})$ tem solução em $\mathbb{Z}$, para todos $e_1, \cdots, e_n \in \mathbb{N}^*$;

(ii) Dado $\varepsilon > 0$, existe $x \in \mathbb{Z}$ tal que $\varphi_{p_i}(x - a_i) < \varepsilon$.

Demonstração:
$(i) \Rightarrow (ii)$ Dado $\varepsilon > 0$, escolha $e_1, \cdots, e_n \in \mathbb{N}$ tais que $p_i^{-e_i} < \varepsilon$. Por hipótese, existe $x \in \mathbb{Z}$ tal que $p_i^{e_i}$ divide $x - a_i$. Assim podemos escrever $x - a_i = p_i^{e_i+\alpha_i}u$, com $\alpha_i \in \mathbb{N}$, $u \in \mathbb{Z}$ e $p_i \nmid u$. Segue que $\varphi_{p_i}(x - a_i) = p_i^{-(e_i+\alpha)} \leq p_i^{-e_i} < \varepsilon$.
$(ii) \Rightarrow (i)$ Para $\varepsilon = \ min\ \{p_i^{-e_i}; i = 1, \cdots, n\}$ existe $x \in \mathbb{Z}$ tal que $\varphi_{p_i}(x - a_i) < \varepsilon \leq p_i^{-e_i}$, $i = 1, \cdots, n$. Escrevendo $x - a_i = p_i^{\beta_i} \cdot v$ com $\beta_i \in \mathbb{N}$, $v \in \mathbb{Z}$ e $p_i \nmid v$, vem que $p_i^{-\beta_i} = \varphi_{p_i}(x - a_i) < p_i^{-e_i}$ e então $\beta_i \geq e_i$. Portanto $p_i^{e_i}$ divide $x - a_i$, isto é, $x \equiv a_i \ (mod\ p_i^{e_i})$.

■

A tentativa de estender a condição (ii) da Proposição acima para uma classe de valores absolutos em um corpo qualquer, leva ao Teorema da Aproximação para valores absolutos, como veremos no Teorema 2.2.1. Isso significa que o Teorema da Aproximação para valores absolutos é, de certa forma, uma extensão do Teorema Chinês de Restos para corpos. Note que o Teorema Chinês de Restos aplicado a um corpo $\mathbb{K}$ não é eficiente, pois $\mathbb{K}$ só possui ideais comaximais 0 e $\mathbb{K}$.

Precisamos de alguns resultados técnicos para chegar ao Teorema da Aproximação para valores absolutos.

Lema 2.2.1 *Seja φ um valor absoluto de $\mathbb{K}$ não-trivial. Dado $x \in \mathbb{K}$ tal que $\varphi(x) > 1$ temos que $\lim_{m\to\infty} \varphi(\frac{x^m}{x^m+1}) = 1$.*

Demonstração: Como $\varphi(x) > 1$, dado $\varepsilon > 0$ existe $m_0 \in \mathbb{N}$ tal que para todo $m \geq m_0$, $\varphi(x^m) = [\varphi(x)]^m > 1 + \frac{1}{\varepsilon}$, ou ainda, $\varphi(x^m) - 1 > \frac{1}{\varepsilon}$. Pela Proposição 2.1.1, $\varphi(x^m - (-1)) \geq |\varphi(x^m) - \varphi(-1)| = |\varphi(x^m) - 1| \geq \varphi(x^m) - 1 > \frac{1}{\varepsilon}$, ou seja, $\varphi(x^m+1) > \frac{1}{\varepsilon}$, ou ainda, $[\varphi(x^m+1)]^{-1} < \varepsilon$. Note que $| \varphi(\frac{x^m}{x^m+1}) - 1 | = | \frac{\varphi(x^m)}{\varphi(x^m+1)} - 1 |$ $= | \frac{\varphi(x^m)-\varphi(x^m+1)}{\varphi(x^m+1)} | \leq \frac{\varphi(x^m-x^m-1)}{\varphi(x^m+1)} = \frac{1}{\varphi(x^m+1)} < \varepsilon$. Então $\lim_{m\to\infty} \varphi(\frac{x^m}{x^m+1}) = 1$.

■

Lema 2.2.2 *Sejam φ um valor absoluto de $\mathbb{K}$ não-trivial e $x \in \mathbb{K}$ tais que $\varphi(x) < 1$. Então $\lim_{m\to\infty} \varphi(\frac{x^m}{x^m+1}) = 0$.*

Demonstração: Por hipótese $\varphi(x) < 1$. Então, dado $\varepsilon > 0$, existe $m_0 \in \mathbb{N}$ tal que para todo $m \geq m_0$, $\varphi(x^m) = [\varphi(x)]^m < \varepsilon$, ou seja, $\lim_{m\to\infty} \varphi(x^m) = 0$. É claro que $\varphi(x^m + 1) \leq \varphi(x^m) + 1$, donde segue que $\lim_{m\to\infty} \varphi(x^m + 1) \leq 1$. Por outro lado, $\varphi(x^m + 1) = \varphi(x^m - (-1)) \geq | \ \varphi(x^m) - 1 \ |$ pela Proposição 2.1.1. Aplicando limite quando $m \to \infty$ na desigualdade acima e usando o fato da função módulo ser contínua em $\mathbb{R}$, vem que $\lim_{m\to\infty} \varphi(x^m + 1) \geq \lim_{m\to\infty} | \ \varphi(x^m) - 1 \ |$ $= | \ \lim_{m\to\infty} \varphi(x^m) - 1 \ | = | \ -1 \ | = 1$. Portanto $\lim_{m\to\infty} \varphi(x^m + 1) = 1$ e então $\lim_{m\to\infty} \varphi(\frac{x^m}{x^m+1}) = \lim_{m\to\infty} \frac{\varphi(x^m)}{\varphi(x^m+1)} = \frac{0}{1} = 0$.

■

Proposição 2.2.2 *Sejam $\varphi_1, \cdots, \varphi_n$, com $n \geq 2$, valores absolutos de $\mathbb{K}$ não-triviais e dois a dois não-equivalentes. Então existe $x \in \mathbb{K}$ tal que*
$\varphi_1(x) > 1, \varphi_2(x) < 1, \cdots, \varphi_n(x) < 1$.

Demonstração: Provaremos esta Proposição utilizando o processo de indução.
Supomos que $n = 2$. Então φ_1 e φ_2 são valores absolutos de $\mathbb{K}$ não-triviais e não-equivalentes. Pela Proposição 2.1.4, existe $y \in \mathbb{K}$ tal que $\varphi_1(y) < 1$ e $\varphi_2(y) \geq 1$ e existe $z \in \mathbb{K}$ tal que $\varphi_1(z) \geq 1$ e $\varphi_2(z) < 1$. Tomamos $x = \frac{z}{y}$. Segue que $\varphi_1(x) = \varphi_1(\frac{z}{y}) = \varphi_1(z).[\varphi_1(y)]^{-1} > 1$ e $\varphi_2(x) = \varphi_2(z).[\varphi_2(y)]^{-1} < 1$. Supomos que a afirmação seja verdadeira para $n - 1$ e vamos provar que também o é para n, onde $n > 2$. Pela hipótese de indução existe $y \in \mathbb{Z}$ tal que $\varphi_1(y) > 1$,

$\varphi_2(y) < 1, \cdots, \varphi_{n-1}(y) < 1$ e, pelo caso $n = 2$, existe $z \in \mathbb{K}$ tal que $\varphi_1(z) > 1$ e $\varphi_n(z) < 1$. Quando $\varphi_n(y) \leq 1$, temos que $x = y^m z$, para $m \in \mathbb{N}$ suficientemente grande satisfaz $\varphi_1(x) = [\varphi_1(y)]^m.\varphi_1(z) > 1$ e $\varphi_k(x) = [\varphi_k(y)]^m.\varphi_k(z) < 1$, para $k \in \{2, \cdots, n\}$. Vamos então estudar o caso em que $\varphi_n(y) > 1$. Quando $k \in \{1, n\}$ temos que $\varphi_k(y) > 1$. Portanto, pelo Lema 2.2.1, $\lim_{m\to\infty} \varphi_k(\frac{y^m}{y^m+1}) = 1$. No caso em que $k \in \{2, \cdots, n-1\}$, temos que $\varphi_k(y) < 1$. Pelo Lema 2.2.2, temos $\lim_{m\to\infty} \varphi_k(\frac{y^m}{y^m+1}) = 0$. Podemos concluir que, para m suficientemente grande, o elemento $x = \frac{z.y^m}{1+y^m}$ satisfaz $\varphi_k(x) = \varphi_k(\frac{z.y^m}{1+y^m}) = \varphi_k(z) \cdot \varphi_k(\frac{y^m}{1+y^m})$. Segue que $\varphi_1(x) > 1, \varphi_2(x) < 1, \cdots, \varphi_n(x) < 1$.

■

Proposição 2.2.3 *Sejam $\varphi_1, \cdots, \varphi_n$, com $n \geq 2$, valores absolutos de $\mathbb{K}$ não-triviais e dois a dois não-equivalentes. Então dado $\varepsilon > 0$, existe $y \in \mathbb{K}$ tal que $\varphi_1(y-1) < \varepsilon, \varphi_2(y) < \varepsilon, \cdots, \varphi_n(y) < \varepsilon$.*

Demonstração: Pela Proposição 2.2.2, existe $x \in \mathbb{K}$ tal que $\varphi_1(x) > 1$, $\varphi_2(x) < 1, \cdots, \varphi_n(x) < 1$. De acordo com com o que vimos na demonstração do Lema 2.2.1, $\lim_{m\to\infty} \varphi_1(\frac{x^m}{1+x^m} - 1) = 0$ e pelo Lema 2.2.2 $\lim_{m\to\infty} \varphi_k(\frac{x^m}{1+x^m}) = 0$ quando $k \in \{2, \cdots n\}$, ou seja, dado $\varepsilon > 0$, existe $m_0 \in \mathbb{N}$ tal que para todo $m \geq m_0$ temos $\varphi_1(\frac{x^m}{1+x^m} - 1) = \mid \varphi_1(\frac{x^m}{1+x^m} - 1) \mid < \varepsilon$ e $\varphi_k(\frac{x^m}{1+x^m}) = \mid \varphi_k(\frac{x^m}{1+x^m}) \mid < \varepsilon$, onde $k \in \{2, \cdots, n\}$. Tomamos $y = \frac{x^m}{1+x^m}$, para m suficientemente grande. Temos que $\varphi_1(y-1) < \varepsilon$ e $\varphi_2(y) < \varepsilon, \cdots, \varphi_n(y) < \varepsilon$.

■

Agora provaremos o Teorema da Aproximação para valores absolutos, devido a Artin e Whaples [1].

Teorema 2.2.1 (Teorema da Aproximação para Valores Absolutos) *Sejam $\varphi_1, \cdots, \varphi_n$ valores absolutos de $\mathbb{K}$ não-triviais e dois a dois não-equivalentes. Dados $x_1, \cdots, x_n \in \mathbb{K}$ e $\varepsilon > 0$, existe $x \in \mathbb{K}$ tal que $\varphi_k(x - x_k) < \varepsilon$ para $k \in \{1, \cdots, n\}$.*

Demonstração: Dados $x_1, \cdots, x_n \in \mathbb{K}$ seja $\rho > max\{\varphi_k(x_j); j,k = 1, \cdots, n\}$. Consideramos o Índice de Kronecker, que é dado por $\delta_{jk} = \begin{cases} 0 \text{ se } j \neq k \\ 1 \text{ se } j = k \end{cases}$. Pela Proposição 2.2.3, existem $y_1, \cdots, y_n \in \mathbb{K}$ tais que $\varphi_k(y_j - \delta_{jk}) < \varepsilon(n.\rho)^{-1}$, onde $j,k \in \{1, \cdots, n\}$. Tomamos $x = \sum_{j=1}^{n} x_j y_j$. Então, $\varphi_k(x - x_k) = \varphi_k((\sum_{j=1}^{n} x_j y_j) - x_k) = \varphi_k(\sum_{j=1}^{n} x_j y_j - x_j\delta_{jk}) \leq \sum_{j=1}^{n} \varphi_k(x_j y_j - x_j\delta_{jk}) = \sum_{j=1}^{n} \varphi_k(x_j(y_j - \delta_{jk})) = \sum_{j=1}^{n} (\varphi_k(x_j).\varphi_k(y_j - \delta_{jk})) < n\rho\varepsilon(n\rho)^{-1} = \varepsilon$.

■

Uma formulação topológica do Teorema da Aproximação para valores absolutos será estudada na próxima seção.

Trabalhando com uma classe de valores absolutos do corpo $\mathbb{K}$, ainda mais particular que aquela do Teorema 2.2.1, apresentaremos uma versão forte do Teorema da Aproximação para valores absolutos. Esta versão possibilita construir uma ordem para o corpo $\mathbb{K}$, como veremos no Corolário 2.2.2.

Lembramos que um subanel D de $\mathbb{K}$ é uma ordem para $\mathbb{K}$ quando $\mathbb{K} = \{ab^{-1}; ab \in D \text{ e } b \neq 0\}$, isto é, se $\mathbb{K}$ é o corpo de frações de D.

Teorema 2.2.2 (Teorema da Aproximação (Versão Forte)) *Seja $\{\varphi_j\}_{j\in J}$ uma família de valores absolutos do corpo $\mathbb{K}$, não-triviais, dois a dois não-equivalentes e não-arquimedianos, com as seguintes propriedades:*

(a) *Para todo $a \in \mathbb{K}$, $a \neq 0$, temos que $\varphi_j(a) = 1$ para quase todo $j \in J$;*

(b) *Dados $j_1, j_2 \in J$, com $j_1 \neq j_2$, para cada $\varepsilon > 0$ existe $a \in \mathbb{K}$ tal que $\varphi_{j_1}(a - 1) < \varepsilon$, $\varphi_{j_2}(a) < \varepsilon$ e $\varphi_j(a) \leq 1$ para todo $j \in J \backslash \{j_1, j_2\}$.*

Sejam $I \subseteq J$, I finito, e $\{a_i\}_{i\in I} \subseteq \mathbb{K}$. Então, para cada $\varepsilon > 0$, existe $a \in \mathbb{K}$ tal que $\varphi_i(a - a_i) < \varepsilon$ para todo $i \in I$, e $\varphi_j(a) \leq 1$ para todo $j \in J \backslash I$.

Demonstração: Podemos assumir que $0 < \varepsilon \leq 1$. Afirmamos que também podemos assumir que I tem pelo menos dois elementos. De fato, se $I = \emptyset$ tomamos

$a = 0$. Se $I = \{i_1\} = J$ tomamos $a = a_{i_1}$. Se $I = \{i_1\}$ e $I \neq J$ temos $i_2 \in J\backslash I$ e escolhemos $I_0 = \{i_1, i_2\}$. Para provar nossa afirmação basta mostrar que se o Teorema vale I_0 então também vale para I. Considerando que o Teorema vale para I_0 temos, para cada $0 < \varepsilon \leq 1$ e cada $\{a_{i_1}, a_{i_2}\} \subseteq \mathbb{K}$, um elemento $a \in \mathbb{K}$ tal que $\varphi_{i_1}(a - a_{i_1}) < \varepsilon$, $\varphi_{i_2}(a - a_{i_2}) < \varepsilon$ e $\varphi_j(a) \leq 1$ para $j \in J\backslash I_0$. Tomando $a_{i_2} = 0$ e notando que $J\backslash I_0 \subseteq J\backslash I$, segue que o Teorema vale para I. Isso mostra nossa afirmação e, portanto, podemos assumir que I possui, no mínimo, dois elementos. Seja $I' = \{j \in J\backslash I; \varphi_j(a_k) > 1$, para pelo menos um $k \in I\}$ e como $\{\varphi_j\}_{j\in J}$ satisfaz a propriedade de (a), vem que para cada $i \in I$, só ocorre $\varphi_j(a_i) > 1$ para uma quantidade finita de $j \in I$. Mas I é finito, e então I' é finito ou vazio. Seja $I_1 = I \cup I'$. Logo, I_1 é finito e tem, no mínimo, dois elementos. Dada a família $\{a_i\}_{i\in I} \subseteq \mathbb{K}$, completamos para obter uma família $\{a_i\}_{i\in I_1}$ tomando $a_i = 0$ para $i \in I'$. Sejam $i \in I_1$ e $j \in J\backslash I_1$. Se $i \in I$ e $j \in J\backslash I_1$ então $\varphi_j(a_i) \leq 1$. Se $i \in I'$ e $j \in J\backslash I_1$ temos que $\varphi_j(a_i) = \varphi_j(0) = 0 \leq 1$. Logo, $\varphi_j(a_i) \leq 1$ para todo $i \in I_1$ e todo $j \in J\backslash I_1$. Vamos mostrar que o Teorema é verdadeiro para I_1. Sejam $M = \max_{i\in I_1}\{\varphi_i(a_i)\}$ e $k \in I_1$. Como $\{\varphi_j\}_{j\in J}$ satisfaz a condição (b), para $k' \in I_1\backslash\{k\}$, existe $b_{kk'} \in \mathbb{K}$ tal que

(1) $\varphi_k(b_{kk'} - 1) < \frac{\varepsilon}{M+1}$,

(2) $\varphi_{k'}(b_{kk'}) < \frac{\varepsilon}{M+1}$,

(3) $\varphi_j(b_{kk'}) \leq 1$ para todo $j \in J\backslash\{k, k'\}$.

Tomando $b_k = \prod_{k'\in I_1\backslash\{k\}} b_{kk'}$ vamos verificar que

(1') $\varphi_k(b_k - 1) < \frac{\varepsilon}{M+1}$,

(2') $\varphi_{k'}(b_k) < \frac{\varepsilon}{M+1}$ para todo $k' \in I_1\backslash\{k\}$,

(3') $\varphi_j(b_k) \leq 1$ para todo $j \in J$.

- (1') : Como φ_k é não-arquimediano temos que $\varphi_k(b_k - 1) = \max\{\varphi_k(b_k), \varphi_k(-1)\} = \max\{\varphi_k(\prod_{k'\in I_1\backslash\{k\}} b_{kk'}), 1\} = \max\{\prod_{k'\in I_1\backslash\{k\}} \varphi_k(b_{kk'}), \prod_{k'\in I_1\backslash\{k\}} 1\} = \prod_{k'\in I_1\backslash\{k\}} \max\{\varphi_k(b_{kk'}), \varphi_k(-1)\}$. Observe que se $b_{kk'} = \pm 1$ para algum $k' \in I_1\backslash\{k\}$ então este fator $b_{kk'}$ não contribui em nada quando tomamos $\varphi_k(b_k) =$

$\prod_{k' \in I_1 \setminus \{k\}} \varphi_k(b_{kk'})$. Como queremos avaliar $\varphi_k(b_k - 1)$ podemos assumir $b_{kk'} \neq \pm 1$ para todo $k' \in I_1 \setminus \{k\}$. Então $\varphi_k(b_k - 1) = \prod_{k' \in I_1 \setminus \{k\}} \varphi_k(b_{kk'} - 1) < \prod_{k' \in I_1 \setminus \{k\}} \frac{\varepsilon}{M+1} \leq \frac{\varepsilon}{M+1}$, pois $\frac{\varepsilon}{M+1} < 1$. Assim, $\varphi_k(b_k - 1) < \frac{\varepsilon}{M+1}$.

- (2') : Note que (2') segue de (2) pois $\varphi'_k(b_k) = \varphi'_k(\prod_{k' \in I_1 \setminus \{k\}} b_{kk'}) = \prod_{k' \in I_1 \setminus \{k\}} \varphi'_k(b_{kk'}) < \prod_{k' \in I_1 \setminus \{k\}} \frac{\varepsilon}{M+1} \leq 1$.

- (3') : Para $j \in J \setminus \{kk'\}$ temos que (3') segue de (3) de forma análoga ao feito no item (2'). Para $j = k'$ temos que (3') segue de (2) pois $\frac{\varepsilon}{M+1} \leq 1$. Falta analisar o caso $j = k$. Pelo mesmo motivo apresentado no item (1'), podemos assumir que $b_{kk'} \neq \pm 1$ para todo $k' \in I_1 \setminus \{k\}$. Segue da Proposição 2.1.5 e de (1) que $\varphi_k(b_{kk'} - 1) = \max\{\varphi_k(b_{kk'}, 1\} < \frac{\varepsilon}{M+1} \leq 1$, implicando em $\varphi_k(b_{kk'}) < 1$. Portanto, $\varphi_k(b_k) < 1$ e temos provado (3').

Tomamos $a = \sum_{k \in I_1} a_k b_k$. Seja $i \in I_1$. Segue que $\varphi_i(a - a_i) = \varphi_i(\sum_{k \in I_1} a_k b_k - a_i) = \varphi_i(\sum_{k \in I_1 \setminus \{i\}} a_k b_k - a_i(b_i - 1))$. Por hipótese os valores absolutos são não-arquimedianos. Então $\varphi_i(a - a_i) \leq \max_{k \in I_1 \setminus \{i\}}\{\varphi_i(a_k)\varphi_i(b_k), \varphi_i(a_i)\varphi_i(b_i - 1)\} < M\frac{\varepsilon}{M+1} < \varepsilon$. Seja $j \in J \setminus I_1$. Então $\varphi_j(a) = \varphi_j(\sum_{k \in I_1} a_k b_k) \leq \max_{k \in I_1 \setminus \{i\}}\{\varphi_j(a_k)\varphi_j(b_k)\} \leq 1$. Assim, $\varphi_i(a - a_i) < \varepsilon$ para todo $i \in I_1$ e $\varphi_j(a) \leq 1$ para todo $j \in J \setminus I_1$, isto é, o Teorema é válido para I_1. Para ver que o Teorema vale para I, observe primeiro que de $a \in \mathbb{K}$ e $\varphi_i(a - a_i) < \varepsilon$ para todo $i \in I_1$, vem imediatamente que $\varphi_i(a - a_i) < \varepsilon$ para todo $i \in I$. Seja $j \in J \setminus I$. Se $j \notin I'$ então $j \in J \setminus I_1$ e temos $\varphi_j(a) \leq 1$. Se $j \in I'$ então $a_j = 0$, $j \in I_1$ e então $\varphi_j(a) = \varphi_j(a - a_j) < \varepsilon \leq 1$.

■

Corolário 2.2.1 *Sejam $\{\varphi_j\}_{j \in J}$ e I como no Teorema 2.2.2. Dada $\{a_j\}_{j \in J} \subseteq \mathbb{K}$ tal que $\varphi_j(a_j) = 1$ para quase todo $j \in J$, existe $a \in \mathbb{K}$ tal que $\varphi_i(a) = \varphi_i(a_i)$ para $i \in I$ e $\varphi_j(a) \leq \varphi_j(a_j)$ para $j \in J \setminus I$.*

Demonstração: Seja $I' = \{j \in J \setminus I; \varphi_j(a_j) \neq 1\}$. Tomamos $I_1 = I \cup I'$. Sendo que I e I' são finitos, temos que I_1 também o é e $\varphi_j(a_j) = 1$ para todo $j \in J \setminus I_1$. Seja $\varepsilon = \min_{i \in I_1}\{\varphi_i(a_i)\}$. Pelo Teorema 2.2.2, existe $a \in \mathbb{K}$ tal que $\varphi_i(a - a_i) < \varepsilon \leq$

$\varphi_i(a_i)$ para $i \in I_1$ e $\varphi_j(a) \leq 1 = \varphi_j(a_j)$ para todo $j \in J \backslash I_1$. Como $\varphi_i(a - a_i) < \varphi_i(a_i)$ vem que $a - a_i \neq a_i$ e $\max\{\varphi_i(a - a_i), \varphi_i(a_i)\} = \varphi_i(a_i)$. Como φ_i é não-arquimediano, usamos a Proposição 2.1.5 e então para todo $i \in I_1$ temos que $\varphi_i(a) =$ $= \varphi_i(a - a_i + a_i) = \max\{\varphi_i(a - a_i), \varphi_i(a_i)\} = \varphi_i(a_i)$. Precisamos ainda, verificar que o Corolário vale para I. Sendo que $\varphi_i(a) = \varphi_i(a_i)$ para todo $i \in I_1$, temos que $\varphi_i(a) = \varphi_i(a_i)$ para todo $i \in I$. Seja $j \in J \backslash I$. Se $j \notin I'$ então $j \notin I_1$, donde segue que $\varphi_j(a) \leq \varphi_j(a_j)$ para todo $j \in J \backslash I$. Se $j \in I'$ então $a_j = 0$ e, pelo Teorema acima, $\varphi_j(a) = \varphi_j(a - a_j) \leq 1 = \varphi_j(a_j)$ para todo $j \in J \backslash I$.

■

Corolário 2.2.2 *Sejam $\{\varphi_j\}_{j \in J}$ como no Teorema 2.2.2. Então $\vartheta = \{a \in \mathbb{K}; \varphi_j(a) \leq 1$ para todo $j \in J\}$ é uma ordem para $\mathbb{K}$.*

Demonstração: Sejam $a, b \in \vartheta$. Então $\varphi_j(ab) = \varphi_j(a)\varphi_j(b) \leq 1$ e $\varphi_j(a + b) \leq \text{máx}\{\varphi_j(a), \varphi_j(b)\} \leq 1$ para todo $j \in J$. Daí $ab \in \vartheta$ e $a + b \in \vartheta$, donde ϑ é subanel de $\mathbb{K}$. Além disto, $\vartheta \neq \emptyset$, pois $0 \in \vartheta$. Seja $j_o \in J$. Como φ_{j_0} é não-trivial, existe $a \in \mathbb{K}$ tal que $\varphi_{j_0}(a) > 1$, donde $\vartheta \neq \mathbb{K}$. Assim, ϑ é subanel próprio de $\mathbb{K}$. A inclusão $\{xy^{-1}; x, y \in \vartheta, y \neq 0\} \subseteq \mathbb{K}$ é óbvia. Para a outra inclusão tomamos $b \in \mathbb{K}$. Se $b = 0$ então $b = 0.1^{-1}$ com $0, 1 \in \vartheta$. Se $b \in \mathbb{K}^*$, consideramos $I = \{j \in J; \varphi_j(b) > 1\}$. Daí, I é finito. Considere a família $\{a_j\}_{j \in J} \subseteq \mathbb{K}$ definida por $a_i = \frac{1}{b}$ se $i \in I$ e $a_j = 1$ se $j \in J \backslash I$. Pelo Corolário 2.2.1, existe $a \in \mathbb{K}$ tal que $\varphi_j(a) \leq \varphi_j(1) = 1$ para $j \in J \backslash I$ e $\varphi_i(a) = \varphi_i(\frac{1}{b}) \leq 1$ para $i \in I$, pois $\varphi_i(b) > 1$. Note que $a \neq 0$ pois $\varphi_i(a) = \varphi_i(\frac{1}{b})$ e $b \neq 0$. Assim, $\varphi_j(a) \leq 1$ para todo $j \in J$, isto é, $a \in \vartheta$. Por outro lado, $\varphi_i(ab) = \varphi_i(a)\varphi_i(b) = 1$ para $i \in I$ e $\varphi_j(ab) \leq 1$ para $j \in J \backslash I$, ou seja, $ab \in \vartheta$. Assim, podemos escrever b como $b = aba^{-1}$, donde ϑ é uma ordem para $\mathbb{K}$.

■

A motivação para estudarmos o Teorema 2.2.2 citado acima, foi dada pelo Exemplo que veremos a seguir. Tal Exemplo envolve os valores absolutos p-ádicos de $\mathbb{Q}$ e permite-nos obter a ordem $\mathbb{Z}$ de $\mathbb{Q}$.

Como vimos no Exemplo 3, citado no início deste capítulo, os valores absolutos p-ádicos de $\mathbb{Q}$ são não-arquimedianos. Além disto, eles são não-triviais e, pelo Exemplo 2, dados p_1 e p_2 primos distintos, temos que φ_{p_1} não é equivalente a φ_{p_2}. Dado $r \in \mathbb{Q}$, $r \neq 0$, temos que $\varphi_p(r) = 1$ para quase todo $p \in \mathbb{Z}$, onde p é primo. Sabendo que r pode ser escrito como $r = \pm p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, onde p_i são primos e $e_i \in \mathbb{Z}$ para $i \in \{1, \cdots, k\}$, temos que $\varphi_p(r) = 1$ quando $p \neq p_i$ para todo $i \in \{1, \cdots, k\}$. Sejam $p_1, p_2 \in \mathbb{Z}$, ambos primos, e $\varepsilon > 0$. Tomamos e como sendo um número inteiro positivo maior que $-\frac{ln\varepsilon}{lnp_i}$ para $i = 1, 2$. Pela Identidade de Bezout, existem $a, b \in \mathbb{Z}$ tais que $ap_1^e + bp_2^e = 1$. Tomamos $r = 1 - ap_1^e = bp_2^e$. Sendo que a pode ser escrito como $a = a'p_1^\alpha$, onde $\alpha, a' \in \mathbb{Z}$, temos que $\varphi_{p_1}(r-1) = \varphi_{p_1}(ap_1^e) = p_1^{-(e+\alpha)} < p_1^{-e} < p_1^{\frac{\ln\varepsilon}{\ln p_1}}$. Mas, $\ln(p_1^{\frac{\ln\varepsilon}{\ln p_1}}) = \frac{\ln\varepsilon}{\ln p_1} \cdot \ln p_1 = \ln\varepsilon$, donde $p_1^{\frac{\ln\varepsilon}{\ln p_1}} = \varepsilon$ e, portanto, $\varphi_{p_1}(r-1) < \varepsilon$. Temos também que $\varphi_{p_2}(r) = \varphi_{p_2}(bp_2^e)$ e, como b pode ser escrito na forma $b = b'p_2^\beta$, com $b', \beta \in \mathbb{Z}$, segue que $\varphi_{p_2}(r) = p_2^{-(e+\beta)} < p_2^{-e} < p_2^{\frac{ln\varepsilon}{\ln p_2}}$. De forma análoga ao que fizemos acima, concluimos que $\varphi_{p_2}(r) < \varepsilon$. Sendo que $\varphi_p(r) = \varphi_p(bp_2^e))$, temos que

$$\varphi_p(r) = \begin{cases} 1, & \text{se} \quad b \text{ não é múltiplo de } p_2 \\ p^{-\alpha}, & \text{se} \quad b = b'p_2^\beta, \text{ com } \alpha = \beta + e \end{cases},$$

para p primo, $p \neq p_1, p_2$ e daí, $\varphi_p(r) \leq 1$. Portanto, o r tomado acima satisfaz a Propriedade (b) do Teorema e, com isso, conclui-se que os valores absolutos p-ádicos satisfazem as hipóteses do Teorema 2.2.2. Sendo $\varphi_{p_1}(r-1) \leq 1$, temos pelo Teorema 2.1.2, que $\varphi_{p_1}(r) \leq 1$. Assim, $\mathbb{Z} = \{r \in \mathbb{Q}; \varphi_p(r) \leq 1 \text{ para todo } p \text{ primo}\}$, o que significa, pelo Corolário 2.2.2, que $\mathbb{Z}$ é uma ordem para $\mathbb{Q}$.

2.3 Corpos Topológicos

Nesta seção veremos que os valores absolutos de um corpo $\mathbb{K}$, são ferramentas eficientes para tornar $\mathbb{K}$ um corpo topológico, isto é, um corpo onde as operações são funções contínuas. Usando alguns resultados sobre corpos topológicos, provaremos

uma versão topológica do Teorema de Aproximação para valores absolutos.

Iniciaremos verificando que um valor absoluto em $\mathbb{K}$ define uma topologia de Hausdorff sobre $\mathbb{K}$ e que esta topologia é discreta exatamente quando o valor absoluto é trivial.

Proposição 2.3.1 *Seja φ um valor absoluto de $\mathbb{K}$. A função $d_\varphi(x,y) = \varphi(x-y)$, para todo $x, y \in \mathbb{K}$, é uma métrica em $\mathbb{K}$.*

Demonstração: Sejam $x, y, z \in \mathbb{K}$.

1. É claro que $d_\varphi(x,y) = \varphi(x-y) \geq 0$. Além disso, $d_\varphi(x,y) = 0$ se, e somente se, $\varphi(x-y) = 0$. Daí, $d_\varphi(x,y) = 0$ se, e somente se, $x = y$.

2. $d_\varphi(x,y) = \varphi(x-y) = \varphi(-(x-y)) = \varphi(y-x) = d_\varphi(y,x)$.

3. $d_\varphi(x,z) = \varphi(x-z) = \varphi(x-y+y-z) \leq \varphi(x-y)+\varphi(y-z) = d_\varphi(x,y)+d_\varphi(y,z)$.

Portanto, d_φ é uma métrica em $\mathbb{K}$.

■

Denotando por ζ_φ a coleção de conjuntos abertos do espaço métrico $(\mathbb{K}, d_\varphi)$, temos que $(\mathbb{K}, \zeta_\varphi)$ é um espaço topológico de Hausdorff. De fato, dados $x, y \in \mathbb{K}$ e $\varepsilon = \frac{d_\varphi(x,y)}{3}$, temos que $x \in B(x,\varepsilon)$, $y \in B(y,\varepsilon)$ e $B(x,\varepsilon) \cap B(y,\varepsilon) = \emptyset$.

Lembramos que uma topologia ζ sobre um conjunto E é chamada de Topologia Discreta quando todos os subconjuntos de E são abertos. Neste caso (E, ζ) é espaço topológico discreto.

Proposição 2.3.2 *Seja φ um valor absoluto do corpo $\mathbb{K}$. A topologia ζ_φ é discreta se, e somente se, φ é o valor absoluto trivial.*

Demonstração: Se ζ_φ é discreta então $\{0\}$ é aberto. Logo, existe $\varepsilon > 0$ tal que $B(0,\varepsilon) = \{0\}$, ou seja, $\varphi(a) < \varepsilon$ se, e somente se, $a = 0$. Seja $x \in \mathbb{K}^*$. Então existe $x^{-1} \in \mathbb{K}^*$ tal que $1 = xx^{-1}$, donde $1 = \varphi(1) = \varphi(x).\varphi(x^{-1})$. Supomos que

$\varphi(x) \neq 1$. Então, ou $\varphi(x) > 1$ ou $\varphi(x) < 1$. Se $\varphi(x) < 1$ então existe $n \in \mathbb{N}$ tal que $\varphi(x^n) = [\varphi(x)]^n < \varepsilon$, donde $x^n = 0$, ou seja $x = 0$, o que é absurdo. Por outro lado, se $\varphi(x) > 1$, ou ainda, $\varphi(x^{-1}) < 1$, então, como feito acima, existe $n \in \mathbb{N}$ tal que $(x^{-1})^n = 0$, o que também é absurdo. Logo, $\varphi(x) = 1$. Concluímos que φ é o valor absoluto trivial. Reciprocamente, se φ é o valor absoluto trivial temos que $d_\varphi(x,y) = \varphi(x-y) = \begin{cases} 0, & \text{se } x = y \\ 1, & \text{se } x \neq y \end{cases}$ $\forall x, y \in \mathbb{K}$. Sejam $\varepsilon = \frac{1}{3}$ e $E \subseteq \mathbb{K}$. Para cada $x \in E$, $\{x\} = B(x, \varepsilon)$ que é aberto. Logo $\{x\}$ é aberto, donde $E = \bigcup_{x \in E} \{x\}$ é aberto, ou seja, todo conjunto de $\mathbb{K}$ é aberto. Portanto ζ_φ é discreta.

■

Nosso próximo passo é verificar que valores absolutos equivalentes geram a mesma topologia em $\mathbb{K}$, e que para cada valor absoluto φ de $\mathbb{K}$ o espaço topológico $(\mathbb{K}, \zeta_\varphi)$, é um corpo topológico. Para isso, recordamos algumas definições.

Definição 2.3.1 *Sejam X e Y espaços topológicos. Uma função $f : X \to Y$ é contínua quando para cada $x \in X$ e cada aberto V de Y contendo $f(x)$ existe um aberto U de X contendo x tal que $f(U) \subseteq V$. Se f é uma bijeção contínua e f^{-1} também é contínua, dizemos que f é um homeomorfismo.*

Verificar que $f : X \to Y$ é contínua é equivalente a mostrar que $f^{-1}(V)$ é aberto em X para todo aberto $V \subseteq Y$.

Quando ζ e ξ são topologias em X e a aplicação identidade, $i : (\mathbb{K}, \xi) \to (\mathbb{K}, \zeta)$, é contínua, dizemos que ξ é mais fina que ζ. Se i é um homeomorfismo então ξ e ζ são topologias equivalentes. Note que ξ ser mais fina que ζ é o mesmo que $\zeta \subseteq \xi$, e que ξ e ζ são equivalentes quando $\xi = \zeta$.

Proposição 2.3.3 *Sejam φ e ψ valores absolutos de $\mathbb{K}$, não-triviais. Então são equivalentes:*

(i) φ é equivalente à ψ.

(ii) $\zeta_\varphi = \zeta_\psi$.

(iii) ζ_φ *é mais fina que* ζ_ψ.

Demonstração:

$(i) \Rightarrow (ii)$ Mostraremos apenas que $i : (\mathbb{K}, \zeta_\varphi) \to (\mathbb{K}, \zeta_\psi)$ é contínua, já que a continuidade de i^{-1} é análoga. Por hipótese temos que existe $\rho > 0$ ($\rho \in \mathbb{R}$) tal que $\varphi = \psi^\rho$. Sejam $x \in \mathbb{K}$ e $E \in \zeta_\psi$ tal que $x \in E$. Então existe $\varepsilon > 0$ tal que $B_\psi(x, \varepsilon) \subseteq E$. Tomando $\varepsilon' = \varepsilon^\rho$ temos que $B_\varphi(x, \varepsilon') \in \zeta_\varphi$ e $B_\varphi(x, \varepsilon') = \{y \in \mathbb{K}; \varphi(x - y) < \varepsilon^\rho\} = \{y \in \mathbb{K}; \psi(x - y)^\rho < \varepsilon^\rho\} = B_\psi(x, \varepsilon) \subseteq E$. Logo, i é contínua.

$(ii) \Rightarrow (iii)$ Segue imediatamente da hipótese e da definição de mais fina.

$(iii) \Rightarrow (i)$ Pela Proposição 2.1.4, basta mostrar que se $x \in \mathbb{K}$ e $\varphi(x) < 1$ então $\psi(x) < 1$. Como ζ_φ é mais fina que ζ_ψ a aplicação $i : (\mathbb{K}, \zeta_\varphi) \to (\mathbb{K}, \zeta_\psi)$ é contínua. Assim, para o aberto $B_\psi(0, 1) \in \zeta_\psi$ que contém 0, existe um aberto $U \in \zeta_\varphi$ contendo 0 tal que $U \subseteq B_\psi(0, 1)$. Desde que $0 \in U$ existe $\varepsilon > 0$ tal que $B_\varphi(0, \varepsilon) \subseteq U \subseteq B_\psi(0, 1)$, assim $\{y \in \mathbb{K}; \varphi(y) < \varepsilon\} \subseteq \{y \in \mathbb{K}; \psi(y) < 1\}$. Dado $x \in \mathbb{K}$ tal que $\varphi(x) < 1$, existe $n \in \mathbb{N}$ tal que $\varphi(x^n) < \varepsilon$. Então $\psi(x^n) < 1$ e daí $\psi(x) < 1$.

■

Note que, pela Proposição 2.3.3, dados φ e ψ valores absolutos de $\mathbb{K}$, não-triviais e não-equivalentes temos que ζ_φ e ζ_ψ são incomparáveis, ou seja, ζ_φ não é mais fina que ζ_ψ e vice-versa.

Nosso próximo passo é definir a Topologia Produto em $\mathbb{K}_1 \times \cdots \times \mathbb{K}_n$. Com isso poderemos falar em corpo topológico e verificarmos que este pode ser definido através de um valor absoluto.

Sejam E um conjunto não-vazio e β uma família de subconjuntos de E tal que:

(a) $\emptyset, E \in \beta$;

(b) se $B_1, B_2 \in \beta$ então $B_1 \cap B_2 \in \beta$.

Chamamos de ζ o conjunto de todas as reuniões possíveis de membros de β.

Afirmação: ζ é uma topologia sobre E.

- $\emptyset, E \in \beta$, donde $\emptyset, E \in \zeta$.
- Sejam $A, B \in \zeta$. Então $A = \bigcup_{A_i \in \beta} A_i$ e $B = \bigcup_{B_j \in \beta} B_j$. Note que $A \cap B = (\bigcup_{A_i \in \beta} A_i) \cap (\bigcup_{B_j \in \beta} B_j) = \bigcup_{i,j \in J} (A_i \cap B_j)$. Mas, $A_i \cap B_j \in \beta$ para cada i e para cada j. Segue, pela definição de ζ, que $A \cap B \in \zeta$.
- Seja $\{A_i\}_{i \in I}$ uma família de elementos de ζ, onde I é um conjunto de índices. Então, para cada i, $A_i = \bigcup_{B_j \in \beta} B_j$. Segue que $\bigcup_{i \in I} A_i = \bigcup_{i \in I} \bigcup_{B_j \in \beta} B_j$, donde $\bigcup_{i \in I} A_i \in \zeta$.

Portanto, ζ é uma topologia sobre E.

Proposição 2.3.4 *Sejam (E_1, ζ) e (E_2, ξ) espaços topológicos e $\beta = \{A \times B; A \in \zeta e\ B \in \xi\}$. Então β satisfaz as condições (a) e (b) citadas acima, para $E = E_1 \times E_2$.*

Demonstração: Como ζ e ξ são topologias sobre E_1 e E_2, respectivamente, temos que $\emptyset \in \beta$ e $E_1 \times E_2 \in \beta$, o que verifica o item (a). Sejam $C_1, C_2 \in \beta$. Então $C_1 = A_1 \times B_1$ e $C_2 = A_2 \times B_2$. Segue que $C_1 \cap C_2 = (A_1 \times B_1) \cap (A_2 \times B_2) = (A_1 \cap A_2) \times (B_1 \cap B_2)$. Sendo que $(A_1 \cap A_2) \in \zeta$ e $(B_1 \cap B_2) \in \xi$, temos que $(C_1 \cap C_2) \in \beta$, donde o item (b) fica satisfeito.

■

Procedendo como anteriormente, temos que o conjunto das uniões de todos os conjuntos de β é uma topologia sobre $E_1 \times E_2$. A esta topologia damos o nome de Topologia Produto. Note que A é aberto em $E_1 \times E_2$ quando $A = \bigcup_{\alpha \in I} A_\alpha$ onde $A_\alpha = A_{\alpha_1} \times A_{\alpha_2}$ com $A_{\alpha_1} \in \zeta$ e $A_{\alpha_2} \in \xi$.

Definição 2.3.2 *Sejam $\mathbb{K}$ um corpo e ζ uma topologia em $\mathbb{K}$. Dizemos que $(\mathbb{K}, \zeta)$ é um corpo topológico se as aplicações*

- $\mathbb{K} \times \mathbb{K} \to \mathbb{K}, \quad (x, y) \mapsto x - y;$
- $\mathbb{K} \times \mathbb{K} \to \mathbb{K}, \quad (x, y) \mapsto x.y;$
- $\mathbb{K}^* \to \mathbb{K}^*, \quad x \mapsto x^{-1};$

são funções contínuas quando consideramos em $\mathbb{K} \times \mathbb{K}$ *a topologia produto.*

Proposição 2.3.5 *Se* φ *é um valor absoluto do corpo* $\mathbb{K}$ *então* $(\mathbb{K}, \zeta_\varphi)$ *é um corpo topológico.*

Demonstração:

- Sejam $(x_0, y_0) \in \mathbb{K} \times \mathbb{K}$ e $E \in \zeta_\varphi$ tal que $x_0 - y_0 \in E$. Então existe $\varepsilon > 0$ tal que $B_\varphi(x_0 - y_0, \varepsilon) \subseteq E$. Tomando $\delta = \frac{\varepsilon}{2}$ e $B = B_\varphi(x_0, \delta) \times B_\varphi(y_0, \delta)$ vem que B é aberto na topologia produto contendo (x_0, y_0). Além disso, se $(x, y) \in B$ então $\varphi(x - x_0) < \delta$ e $\varphi(y - y_0) < \delta$ implicando em $\varphi(x - y - (x_0 - y_0)) \leq \varphi(x - x_0) + \varphi(y - y_0) < \varepsilon$. Assim, $x - y \in B_\varphi(x_0 - y_0, \varepsilon) \subseteq E$. Segue que a função diferença é contínua.

- Sejam $(x_0, y_0) \in \mathbb{K} \times \mathbb{K}$ e $E \in \zeta_\varphi$ tal que $x_0 y_0 \in E$. Então existe $\varepsilon > 0$ tal que $B_\varphi(x_0 y_0, \varepsilon) \subseteq E$. Tomando $\delta = \frac{1}{2} min\{\sqrt{\varepsilon}, \frac{\varepsilon}{\varphi(x_0)+1}, \frac{\varepsilon}{\varphi(y_0)+1}\}$ e $B = B_\varphi(x_0, \delta) \times B_\varphi(y_0, \delta)$ vem que B é aberto na topologia produto contendo (x_0, y_0). Além disso, se $(x, y) \in B$ então $\varphi(x - x_0) < \delta$ e $\varphi(y - y_0) < \delta$. Note ainda que $\varphi(x - x_0).\varphi(y_0) < \delta \cdot \varphi(y_0) \leq \frac{1}{3} \cdot \frac{\varepsilon}{\varphi(y_0)+1} \cdot \varphi(y_0) < \frac{\varepsilon}{3}$. Analogamente $\varphi(y - y_0) \cdot \varphi(x_0) < \frac{\varepsilon}{3}$. Assim, $\varphi(xy - x_0 y_0) \leq \varphi(x - x_0) \cdot \varphi(y - y_0) + \varphi(x - x_0) \cdot \varphi(y_0) + \varphi(x_0) \cdot \varphi(y - y_0) < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon$. Portanto $xy \in B_\varphi(x_0 y_0, \varepsilon) \subseteq E$. Segue que a função produto é contínua.

- Sejam $x_0 \in \mathbb{K}^*$ e $E \in \zeta_\varphi$ tal que $x_0^{-1} \in E$. Então existe $\varepsilon > 0$ tal que $B_\varphi(x_0^{-1}, \varepsilon) \subseteq E$. Tomando $\delta = \frac{1}{2} \min\{\varphi(x_0), \varepsilon[\varphi(x_0)]^2\}$ e $B = B_\varphi(x_0, \delta)$ vem que B é aberto em ζ_φ contendo x_0. Se $x \in \mathbb{K}^*$ e $x \in B$ então $\varphi(x - x_0) < \delta$. Para mostrar que $x^{-1} \in B_\varphi(x_0^{-1}, \varepsilon) \subseteq E$, separamos a demonstração em dois casos:

Caso 1: $\varphi(x_0) \leq \varphi(x)$, ou ainda, $\varphi(x)^{-1} \leq \varphi(x_0)^{-1}$.

Temos que $\varphi(x^{-1}-x_0^{-1}) = \varphi((x-x_0)(-x_0^{-1}x^{-1})) = \varphi(x-x_0)\varphi(-x_0)^{-1}\varphi(x)^{-1} \leq$ $\varphi(x-x_0)[\varphi(-x_0)^{-1}]^2 < \frac{1}{2}min\{\varphi(x_0), \varepsilon[\varphi(x_0)]^2\}[\varphi(-x_0)^{-1}]^2 \leq$ $\frac{1}{2}\varepsilon[\varphi(x_0)]^2\varphi(x_0)^{-2} < \varepsilon$.

Caso 2: $\varphi(x) < \varphi(x_0)$, ou seja, $\varphi(x)^{-1} > \varphi(x_0)^{-1}$.

Note que $\varphi(x) - \varphi(x_0) < 0$, donde $\mid \varphi(x) - \varphi(x_0) \mid = \varphi(x_0) - \varphi(x)$. Pela Proposição 2.1.1, item (e), $\mid \varphi(x) - \varphi(x_0) \mid \leq \varphi(x - x_0)$, o que implica em $\varphi(x_0) - \varphi(x) \leq \varphi(x - x_0) < \frac{1}{2}min\{\varphi(x_0), \varepsilon[\varphi(x_0)]^2\} \leq \frac{1}{2}\varphi(x_0)$, isto é, $\varphi(x) > \frac{1}{2}\varphi(x_0)$, ou ainda, $\varphi(x)^{-1} < 2\varphi(x_0)^{-1}$. Segue que $\varphi(x^{-1} - x_0^{-1}) = \varphi(x - x_0)\varphi(x_0^{-1})\varphi(x^{-1}) < \varphi(x - x_0)\varphi(x_0^{-1})2\varphi(x_0^{-1}) < \frac{1}{2}\delta 2[\varphi(x_0)]^{-2} < \varepsilon[\varphi(x_0)]^2[\varphi(x_0)]^{-2} = \varepsilon$. Portanto, a função $x \mapsto x^{-1}$ é contínua em x_0, para todo $x_0 \in \mathbb{K}^*$. Logo, tal função é contínua.

Concluímos que $(\mathbb{K}, \zeta)$ é um corpo topológico.

■

Nosso objetivo agora é mostrar que o Teorema da Aproximação (versão 2.2.1) possui uma versão topológica.

Teorema 2.3.1 (Teorema da Aproximação - Versão Topológica) *Sejam $\varphi_1, \cdots, \varphi_n$ valores absolutos de $\mathbb{K}$, não-triviais e dois a dois não-equivalentes. Considere $\mathbb{K}_k = (\mathbb{K}, \zeta_{\varphi_k})$ o corpo topológico munido da topologia ζ_{φ_k} para $k \in \{1, \cdots, n\}$. São equivalentes:*

(*i*) *Dados $x_1, \cdots, x_n \in \mathbb{K}$ e $\varepsilon > 0$, existe $x \in \mathbb{K}$ tal que $\varphi_k(x - x_k) < \varepsilon$, para $k \in \{1, \cdots, n\}$;*

(*ii*) *A imagem de $\mathbb{K}$ pela aplicação diagonal $\nabla : \mathbb{K} \to \mathbb{K}_1 \times \cdots \times \mathbb{K}_n$ é densa no espaço produto.*

Demonstração:

(*i*) $\Rightarrow$ (*ii*) Seja A um aberto de $\mathbb{K}_1 \times \mathbb{K}_2 \times \cdots \times \mathbb{K}_n$. Então $A = \bigcup_{\alpha \in I} A_\alpha$ onde $A_\alpha =$

$A_{\alpha_1} \times A_{\alpha_2} \times \cdots \times A_{\alpha_n}$ e A_{α_i} é aberto no espaço topológico $(\mathbb{K}, \zeta_{\varphi_i})$ e I é um conjunto de índices. Queremos mostrar que $A \cap \nabla(\mathbb{K}) \neq \emptyset$, mas basta mostrar que $A_\alpha \cap \nabla(\mathbb{K}) \neq \emptyset$, pois $A_\alpha \subseteq A$. Sejam $x_i \in A_{\alpha_i}$ onde $i = 1, 2, \cdots, n$. Como A_{α_i} é aberto em $(\mathbb{K}, \zeta_{\varphi_i})$, existe $\varepsilon_i > 0$ tal que $B_{\varphi_i}(x_i, \varepsilon_i) \subseteq A_{\alpha_i}$. Seja $\varepsilon = min\{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n\}$. Então $B_{\varphi_i}(x_i, \varepsilon) \subseteq B_{\varphi_i}(x_i, \varepsilon_i)$, $i = 1, \cdots, n$. Daí, $B_{\varphi_1}(x_1, \varepsilon) \times \cdots \times B_{\varphi_n}(x_n, \varepsilon) \subseteq B_{\varphi_1}(x_1, \varepsilon_1) \times \cdots \times B_{\varphi_n}(x_n, \varepsilon_n) \subseteq A_{\alpha_1} \times \cdots \times A_{\alpha_n} = A_\alpha$. Portanto, basta mostrar que $(B_{\varphi_1}(x_1, \varepsilon) \times \cdots \times B_{\varphi_n}(x_n, \varepsilon)) \cap \nabla(\mathbb{K}) \neq \emptyset$. Para $x_1, \cdots, x_n \in \mathbb{K}$ e $\varepsilon > 0$, usamos a hipótese (i) e obtemos $x \in \mathbb{K}$ tal que $\varphi_i(x - x_i) < \varepsilon$ para $i = 1, \cdots, n$, ou seja, $x \in \mathbb{K}$ e $x \in B_{\varphi_i}(x_i, \varepsilon)$. Então $(x, \cdots, x) \in B_{\varphi_1}(x_1, \varepsilon) \times \cdots \times B_{\varphi_n}(x_n, \varepsilon)$. Mas, $(x, \cdots, x) = \nabla(x) \in \nabla(\mathbb{K})$, ou seja, $(x, \cdots, x) \in \nabla(\mathbb{K}) \cap (B_{\varphi_1}(x_1, \varepsilon) \times \cdots \times B_{\varphi_n}(x_n, \varepsilon))$. Assim, $\nabla(\mathbb{K}) \cap A \neq \emptyset$ e portanto, $\nabla(\mathbb{K})$ é denso em $\mathbb{K}_1 \times \mathbb{K}_2 \times \cdots \times \mathbb{K}_n$.

$(ii) \Rightarrow (i)$ Sejam $x_1, \cdots, x_n \in \mathbb{K}$ e $\varepsilon > 0$. Tomamos $A = B_{\varphi_1}(x_1, \varepsilon) \times \cdots \times B_{\varphi_n}(x_n, \varepsilon)$, o qual é aberto em $\mathbb{K}_1 \times \mathbb{K}_2 \times \cdots \times \mathbb{K}_n$. Por hipótese, $\nabla(\mathbb{K}) \cap A \neq \emptyset$, ou seja, existe $x \in \mathbb{K}$, tal que $\nabla(x) \in A$, ou melhor, $(x, \cdots, x) \in B_{\varphi_1}(x_1, \varepsilon) \times \cdots \times B_{\varphi_n}(x_n, \varepsilon)$. Então, $x \in B_{\varphi_i}(x_i, \varepsilon)$, $i = 1, \cdots, n$. Logo, $\varphi_i(x - x_i) < \varepsilon$, $i = 1, \cdots, n$.

■

2.4 Teorema da Aproximação para Valorizações Exponenciais

Na seção anterior falamos sobre valores absolutos não-arquimedianos. Através deles definiremos as valorizações exponenciais para as quais mostraremos uma versão do Teorema da Aproximação. Antes disso, veremos que as valorizações exponenciais estão em correspondência biunívoca com os valores absolutos não-arquimedianos. Assim, como os valores absolutos p-ádicos atendem a esta Propriedade, obtemos as chamadas valorizações exponenciais p-ádicas.

Recordamos que um valor absoluto não-arquimediano sobre um corpo $\mathbb{K}$ é uma função $\varphi : \mathbb{K} \to \mathbb{R}_+$ satisfazendo:

(VA_1) $\varphi(x) = 0$ se e somente se $x = 0$;

(VA_2) $\varphi(xy) = \varphi(x).\varphi(y)$, para todos $x, y \in \mathbb{K}$;

(VA_4) $\varphi(x+y) \leq max\{\varphi(x), \varphi(y)\}$, para todos $x, y \in \mathbb{K}$.

Assim a condição

(VA_3) $\varphi(x+y) \leq \varphi(x) + \varphi(y)$

não é exigida, e conseqüentemente a adição de $\mathbb{R}$ não é necessária para definir valor absoluto não-arquimediano. Portanto no contra-domínio de φ precisamos somente da estrutura de grupo multiplicativo de $\mathbb{R}_+^*$, com sua relação de ordem natural, e do elemento 0.

É procedimento usual, e às vezes mais conveniente, escrever o contra-domínio de um valor absoluto não-arquimediano com notação aditiva, isto é, trocar o grupo multiplicativo $\mathbb{R}_+^*$ e sua relação de ordem, por um grupo aditivo isomorfo a $\mathbb{R}_+^*$, com uma relação de ordem induzida por este isomorfismo.

Esta troca pode ser feita facilmente observando que:

- $ln(x.y) = ln(x) + ln(y)$, para todos $x, y \in \mathbb{R}_+^*$.
- $x < y \Leftrightarrow ln(x) < ln(y)$, para todos $x, y \in \mathbb{R}_+^*$.

Assim, a função

$$ln : \mathbb{R}_+^* \to \mathbb{R}$$

é um isomorfismo entre grupos $(\mathbb{R}_+^*, .)$ e $(\mathbb{R}, +)$ que induz a relação de ordem usual de $\mathbb{R}$.

Para o valor absoluto não-arquimediano $\varphi : \mathbb{K} \to \mathbb{R}_+$, consideremos a função

$$v : \mathbb{K}^* \to \mathbb{R} \text{ definida por } v = -ln \circ \varphi.$$

Como v não está definida em 0, estendemos v ao corpo $\mathbb{K}$, acrescentando

o símbolo ∞ ao contra-domínio de v e convencionando $\infty = -ln0$. Segue que $v(0) = \infty$. Tomando também por convenção $e^{-\infty} = 0$, obtemos de (VA_1) a seguinte propriedade:

(VE_1) $v(x) = \infty \Leftrightarrow x = 0$.

$(\Rightarrow)$ $v(x) = \infty \Rightarrow -ln(\varphi(x)) = \infty = -ln0$ $(\Leftarrow)$ $x = 0$
$\Rightarrow e^{-ln(\varphi(x))} = e^{-ln0} = e^{-\infty}$ $\Rightarrow v(x) = \infty$.
$\Rightarrow \varphi(x) = 0 \Rightarrow x = 0$

Estamos considerando agora $v : \mathbb{K} \to \mathbb{R} \cup \{\infty\}$, e portanto, precisamos estender a estrutura de grupo aditivo abeliano, bem como a relação de ordem, de $\mathbb{R}$ para $\mathbb{R} \cup \{\infty\}$. Desde que $v(0) = \infty$ e $v(xy) = -ln(\varphi(x)) - ln(\varphi(y))$, as identidades $0 \cdot 0 = u \cdot 0 = 0 \cdot u = 0$, para todo $u \in \mathbb{R}$, sugerem tomarmos $\infty + \infty = u + \infty = \infty + u = \infty$, para todo $u \in \mathbb{R}$. Consideramos ainda, $u < \infty$, para todo $u \in \mathbb{R}$. Desta forma, é fácil ver que $\mathbb{R} \cup \{\infty\}$ é um grupo abeliano aditivo e totalmente ordenado.

As condições (VA_2) e (VA_4) garantem, respectivamente, as seguintes propriedades para v:

(VE_2) $v(x.y) = v(x) + v(y)$, para todo $x, y \in \mathbb{K}$;

(VE_3) $v(x + y) \geq min\{v(x), v(y)\}$, para todo $x, y \in \mathbb{K}$.

De fato, (VE_2) é imediata de (VA_2) para $x, y \in \mathbb{K}^*$. Quando $x = 0$ ou $y = 0$ o resultado segue das convenções $\infty + \infty = u + \infty = \infty + u = \infty$ para todo $u \in \mathbb{R}$. Para verificar (VE_3), consideremos primeiro o caso $x, y, x + y \in \mathbb{K}^*$. Assim $\varphi(x+y) \leq max\{\varphi(x), \varphi(y)\}$ implica em $ln(\varphi(x+y)) \leq ln(max\{\varphi(x), \varphi(y)\}) = max\{ln(\varphi(x)), ln(\varphi(y))\}$, e então, $v(x + y) \geq -max\{ln(\varphi(x)), ln(\varphi(y))\} = min\{-ln(\varphi(x)), -ln(\varphi(y))\} = min\{v(x), v(y)\}$.

Observamos ainda que poderíamos trocar a definição $v = -ln \circ \varphi$ por $v = ln \circ \varphi$, mas neste caso, as condições (VE_1) e (VE_2) deveriam ser repassadas para

$(VE_{1'})$ $v(x) = -\infty$ se, e somente se, $x = 0$,

$(VE_{3'})$ $v(x + y) \leq max\{v(x), v(y)\}$, para todos $x, y \in \mathbb{K}$,

quando consideramos $v : \mathbb{K} \to \mathbb{R} \cup \{-\infty\}$ e as convenções $ln\ 0 = -\infty$, $e^{+\infty} = 0$, $-\infty - \infty = u - \infty = -\infty + u = -\infty$ e $-\infty < u$, para todo $u \in \mathbb{K}$.

Definição 2.4.1 *Uma valorização exponencial de um corpo* $\mathbb{K}$ *é uma aplicação* $v : \mathbb{K} \to \mathbb{R} \cup \{\infty\}$ *satisfazendo as condições* (VE_1), (VE_2) *e* (VE_3), *onde temos as convenções* $\infty + \infty = u + \infty = \infty + u = \infty$ *e* $u < \infty$, *para todo* $u \in \mathbb{R}$.

O procedimento feito anteriormente associa a cada valor absoluto não-arquimediano de $\mathbb{K}$ uma única valorização exponencial. A recíproca deste fato também é verdadeira, como mostra o próximo Teorema.

Teorema 2.4.1 *Seja* $\mathbb{K}$ *um corpo. Existe uma correspondência biunívoca entre valores absolutos não-arquimedianos de* $\mathbb{K}$ *e valorizações exponenciais de* $\mathbb{K}$.

Demonstração: Já vimos que

$$\psi : \{\varphi;\ \varphi \text{é um valor absoluto não-arquimediano de } \mathbb{K}\} \to \{v;\ v \text{é valorização exponencial de } \mathbb{K}\}$$

dada por $\psi(\varphi) = -ln(\varphi)$ é uma função bem definida, isto é, $v = -\ln(\varphi)$ é uma valorização exponencial de $\mathbb{K}$. Claramente a aplicação

$$\widehat{\psi} : \{v;\ v \text{ é valorização exponencial de } \mathbb{K}\} \to \{\varphi;\ \varphi \text{ é um valor absoluto não-arquimediano de } \mathbb{K}\}$$

dada por $\widehat{\psi}(v) = e^{-v}$ satisfaz $\widehat{\psi} \circ \psi = \psi \circ \widehat{\psi} = Id$. Assim, basta mostrar que $\widehat{\psi}$ está bem definida, isto é, mostrar que $\varphi = e^{-v}$ é um valor absoluto não-arquimediano de $\mathbb{K}$. É imediato que $\varphi : \mathbb{K} \to \mathbb{R}_+$, $\varphi(0) = 0$ pela convenção $e^{-\infty} = 0$, e que $\varphi(x) = 0$ implica em $e^{-v(x)} = 0$ daí, $-v(x) = -\infty$ e segue que $x = 0$ por (VE_1). Assim vale (VA_1). A condição (VA_2) é trivialmente verificada. Para mostrar (VA_4) observe que, para $x, y \in \mathbb{K}$ temos $ln(\varphi(x+y)) = -v(x+y) \leq -min\{v(x), v(y)\} = max\{-v(x), -v(y)\}$ e então $\varphi(x+y) \leq e^{max\{-v(x),-v(y)\}} = max\{e^{-v(x)}, e^{-v(y)}\} = max\{\varphi(x), \varphi(y)\}$.

■

Exemplos:

- Seja φ a valorização trivial de $\mathbb{K}$. Já vimos que φ é não-arquimediana. Então, dado $x \in \mathbb{K}$, $\varphi(x) = \begin{cases} 0, & \text{se } x = 0 \\ 1, & \text{se } x \neq 0 \end{cases}$,

temos que $v(x) = -ln(\varphi(x)) = \begin{cases} -ln(0), & \text{se } x = 0 \\ -ln(1), & \text{se } x \neq 0 \end{cases} = \begin{cases} \infty, & \text{se } x = 0 \\ 0, & \text{se } x \neq 0 \end{cases}$.

Definimos então a valorização exponencial trivial como

$$v(x) = \begin{cases} \infty, & \text{se } x = 0, \\ 0, & \text{se } x \neq 0 \end{cases}.$$

Um caso particular da valorização exponencial trivial pode ser visto definindo $v(\overline{0}) = \infty$ e $v(\overline{1}) = 0$, considerando $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$.

- No exemplo 3 citado no início deste capítulo, definimos o valor absoluto p-ádico de $\mathbb{Q}$ como uma aplicação $\varphi_p : \mathbb{Q} \to \mathbb{R}_+$ dada por

$$\varphi_p(x) = \begin{cases} 0, & \text{se } x = 0 \\ p^{-n}, & \text{se } x \neq 0 \end{cases},$$

onde n é dado pela única decomposição de x ($x = \frac{u}{v}p^n$). Mais ainda, verificamos que este é não-arquimediano. Podemos então definir a aplicação $v_p : \mathbb{Q} \to \mathbb{R} \bigcup \{\infty\}$ como $v_p(x) = -ln(\varphi(x)) = \begin{cases} -ln(0), & \text{se } x = 0 \\ -ln(p^{-n}), & \text{se } x \neq 0 \end{cases}$.

Logo,

$$v_p(x) = \begin{cases} \infty, & \text{se } x = 0 \\ ln(p^n), & \text{se } x \neq 0 \end{cases}.$$

Tal função é chamada de valorização exponencial p-ádica de $\mathbb{Q}$.

Para provar o Teorema da Aproximação para valorizações exponenciais usamos, além do Teorema da Aproximação para valores absolutos, a seguinte Proposição:

Proposição 2.4.1 *Sejam $v : \mathbb{K} \to \mathbb{R} \cup \{\infty\}$ uma valorização exponencial e $x, y \in \mathbb{K}$. Se $v(x) \neq v(y)$ então $v(x+y) = min\{v(x), v(y)\}$.*

Demonstração: Seja φ o valor absoluto de $\mathbb{K}$ correspondente a v, isto é, $\varphi(x) = e^{-v(x)}$. De $v(x) \neq v(y)$ vem que $\varphi(x) \neq \varphi(y)$e, pela Proposição 2.1.5, temos que $\varphi(x+y) = max\{\varphi(x), \varphi(y)\}$. Então $v(x+y) = -ln(\varphi(x+y)) = -ln(max\{\varphi(x), \varphi(y)\}) = -max\{ln(\varphi(x)), ln(\varphi(y))\} = min\{-ln(\varphi(x)), -ln(\varphi(y))\} = min\{v(x), v(y)\}$. ■

valores absolutos não arquimedianos

Sejam φ, ψ ~~valorizações não arquimedianas~~ equivalentes. Então existe $\rho \in \mathbb{R}$, $\rho > 0$, tal que $\varphi = \psi^\rho$. Daí, $-ln(\varphi) = -ln(\psi^\rho) = \rho(-ln(\psi))$. Sabemos que existem v, w valorizações exponenciais tais que $v = -ln(\varphi)$ e $w = -ln(\psi)$. Então $v = -ln(\varphi) = \rho(-ln(\psi)) = \rho w$. Podemos então dizer que duas valorizações exponenciais, v e w, são equivalentes quando existe $\rho \in \mathbb{R}$, $\rho > 0$, tal que $v = \rho w$.

Uma última definição:

Se $v : \mathbb{K} \to \mathbb{R} \cup \{\infty\}$ é uma valorização exponencial de $\mathbb{K}$, chamamos de grupo de valores de v ao conjunto $v(\mathbb{K}^*)$. Note que $v(\mathbb{K}^*)$ é um grupo já que v é um homomorfismo de grupos por (VE_2).

Teorema 2.4.2 (Teorema da Aproximação para Valorizações Exponenciais) *Sejam $v_1, \cdots, v_n$ valorizações exponenciais de $\mathbb{K}$, duas a duas não-equivalentes. Então, para cada $x_1, \cdots, x_n \in \mathbb{K}$ e $\gamma_1 \in \Gamma_{v_1}, \cdots, \gamma_n \in \Gamma_{v_n}$ (Γ_{v_i} é o grupo de valores de v_i), existe um $x \in \mathbb{K}$ tal que $v_i(x - x_i) = \gamma_i$ para $i = 1, \cdots, n$.*

Demonstração: Por $v_1, \cdots, v_n$ serem duas a duas não-equivalentes, sabemos que existe, no máximo, uma valorização exponencial trivial (caso nenhuma das valorizações exponenciais acima seja a trivial, podemos acrescentá-la ao conjunto, sem a perda de suas propriedades). Assumimos, sem perda de generalidade, que tal valorização é v_1. Então, $\gamma_1 = 0$. Tomamos $y_2, \cdots, y_n \in \mathbb{K}$ tais que $v_i(y_i) = \gamma_i$ para $i = 2, \cdots, n$. Pela definição de valorização exponencial, $\varphi_i(y_i) = e^{-\gamma_i} > 0$. Pelo Teorema da Aproximação para Valores Absolutos, existe $y \in \mathbb{K}$ tal que $\varphi_i(y - y_i) <$

$e^{-\gamma_i}$. Então $ln(\varphi_i(y-y_i)) < -\gamma_i$. Daí, $v_i(y-y_i) > \gamma_i$ para $i = 2, \cdots, n$. Da mesma forma, existe $z \in \mathbb{K}$ tal que $v_i(z-x_i) > \gamma_i$ para $i = 2, \cdots, n$. Note que y e z devem ser tomados de tal forma que $y+z \neq x_1$ pois, se assim fosse, teríamos que $v_1((y+z)-x_1) = v_1(0) = \infty \neq 0 = \gamma_1$. Segue que, para $i = 2, \cdots, n$, temos $v_i(y) = v_i((y-y_i)+y_i)$. Mas, $v_i(y-y_i) \neq v_i(y)$. Então, pela Proposição 2.4.1, $v_i((y-y_i)+y_i) = min\{v_i(y-y_i), v_i(y_i)\} = \gamma_i$. Então $v_i(y) = \gamma_i$. Da mesma forma, $v_i(y+(z-x_i)) = \gamma_i$. Tomamos $x = y+z$. Então $v_1(x-x_1) = \gamma_1$ e $v_i(x-x_i) = v_i(y+z-x_i) = v_i(y+(z-x_i)) = \gamma_i$ para $i = 2, \cdots, n$. Portanto, existe $x \in \mathbb{K}$ tal que $v_i(x-x_i) = \gamma_i$ para $i = 1, \cdots, n$.

■

Corolário 2.4.1 *Sejam $v_1, \cdots, v_n$ valorizações exponenciais de $\mathbb{K}$, duas a duas não-equivalentes. Para cada $\gamma_i \in \Gamma_{v_i}$, com $i = 1, \cdots, n$, existe um $x \in \mathbb{K}$ tal que $v_i(x) = \gamma_i$ para $i = 1, \cdots, n$.*

Demonstração: Sejam $x_1 = \cdots = x_n = 0 \in \mathbb{K}$. Pelo Teorema 2.4.2, existe $x \in \mathbb{K}$ tal que $v_i(x) = v_i(x-0) = v_i(x-x_i) = \gamma_i$.

■

No próximo capítulo mostraremos o Teorema da Aproximação para valorizações de Krull, que são uma generalização das valorizações exponenciais.

Capítulo 3

Anéis de Valorização e Teorema da Aproximação

O principal objetivo deste capítulo é mostrar o Teorema da Aproximação para Anéis de Valorização. Sendo assim, após definirmos tais anéis falaremos sobre algumas de suas propriedades, as quais permitem-nos enunciar dois resultados importantes: o Teorema da Correspondência e o Teorema da Extensão.

Sendo que no capítulo anterior falamos sobre as valorizações exponenciais, vamos agora generalizar tal conceito, ou seja, falaremos sobre as valorizações de Krull. A partir de tais valorizações podemos relacionar as valorizações de um corpo com os anéis de valorização do mesmo.

As definições de sistema multiplicativo e de Anéis de Prüfer, bem como alguns resultados envolvendo tais conceitos são usados para demonstrar o que chamamos de versão fraca do Teorema da Aproximação para anéis de valorização. Para provar a versão forte de tal Teorema, precisamos ainda da definição de valorizações independentes.

3.1 Anéis de Valorização

Esta primeira seção tem por objetivo apresentar a definição de Anéis de Valorização, bem como estudar alguns resultados que envolvem tal conceito.

Definição 3.1.1 *Sejam $\mathbb{K}$ um corpo e A um subanel de $\mathbb{K}$. Dizemos que A é um anel de valorização de $\mathbb{K}$ se, para todo $x \in \mathbb{K}\backslash\{0\}$, temos que $x \in A$ ou $x^{-1} \in A$.*

Observações:

- Se A é anel de valorização de $\mathbb{K}$ então A é um subdomínio de $\mathbb{K}$.
- $\mathbb{K}$ é anel de valorização de $\mathbb{K}$.
- $\mathbb{K}$ é o corpo quociente de A, quando A é um anel de valorização de $\mathbb{K}$. De fato, dado $x \in \mathbb{K}$ temos para $x = 0$ que $x = 0 \cdot 1^{-1}$ com $0, 1 \in A$. Para $x \neq 0$ e $x \in A$ temos $x = x \cdot 1^{-1}$ com $x, 1 \in A$. Para $x \neq 0$ e $x^{-1} \in A$ temos $x = 1 \cdot (x^{-1})^{-1}$ com $1, x^{-1} \in A$.

Note que não vale a recíproca da observação acima. Por exemplo, $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$, mas $\mathbb{Z}$ não é anel de valorização de $\mathbb{Q}$, já que $\frac{3}{2}$ e $\frac{2}{3}$ não estão em $\mathbb{Z}$.

Para apresentar exemplos de corpos que possuem anel de valorização próprio, precisamos excluir os corpos que são extensões algébricas de um corpo finito, conforme resultado abaixo.

Lema 3.1.1 *Seja $\mathbb{K}$ um corpo.*

(a) *Se $\mathbb{K}$ é finito então $\mathbb{K}$ não possui anel de valorização próprio.*

(b) *Se $\mathbb{K}$ é uma extensão algébrica de um corpo finito então $\mathbb{K}$ não possui anel de valorização próprio.*

Demonstração:

(a) Se V é uma anel de valorização de $\mathbb{K}$ então $(V,+)$ é um subgrupo de $(\mathbb{K},+)$. Vamos admitir que $\mid \mathbb{K} \mid = n = 2+2k+r$ e escrever

$\mathbb{K} = \{0,1,x_1,\cdots,x_r,y_1,y_2,\cdots,y_{2k-1},y_{2k}\}$ onde $x_j \cdot x_j = y_i \cdot y_{i+1} = 1$, para $j \in \{1,2,\cdots,r\}$ e $i \in \{1,3,\cdots,2k-1\}$, isto é, x_j tem ordem 2 em $(\mathbb{K}^*,\cdot)$ e y_{i+1} é o inverso de y_i em $(\mathbb{K}^*,\cdot)$. Desde que V é anel de valorização de $\mathbb{K}$ devemos ter $0,1,x_1,\cdots,x_r \in V$ e, além disso, $y_i \in V$ ou $y_{i+1} \in V$ para $i = 1,3,\cdots,2k-1$. Segue que V tem pelo menos $2+r+k$ elementos. Como $\mathbb{K}$ tem $2+r+2k$ elementos, usamos o Teorema de Lagrange para concluir que $\mid V \mid = \mid \mathbb{K} \mid$ e portanto $V = \mathbb{K}$.

(b) Assuma que $\mathbb{K}$ seja extensão algébrica de $\mathbb{K}_0$, $\mathbb{K}_0$ um corpo finito, e V um anel de valorização de $\mathbb{K}$. É fácil ver que $A = V \cap \mathbb{K}_0$ é anel de valorização de $\mathbb{K}_0$, e pelo item (a), temos que $A = \mathbb{K}_0$. Logo $\mathbb{K}_0 \subseteq V$. Se $\mathbb{K}_0 = V$ então V é corpo. Mas $\mathbb{K}$ é o corpo de frações de V, e então $\mathbb{K} = V$. Se $\mathbb{K}_0 \subsetneq V \subseteq \mathbb{K}$, tome $\alpha \in \mathbb{K}$. Se $\alpha \in V$ então $\mathbb{K} = V$ e se $\alpha^{-1} \in V$ temos $\mathbb{K}_0[\alpha^{-1}] \subseteq V$. Como $\mathbb{K}$ é algébrico sobre $\mathbb{K}_0$ e $\alpha^{-1} \in \mathbb{K}$ temos que $\mathbb{K}_0[\alpha^{-1}]$ é corpo contendo α^{-1}. Segue que $\alpha = (\alpha^{-1})^{-1} \in \mathbb{K}_0[\alpha^{-1}] \subseteq V$. Portanto, $V = \mathbb{K}$.

■

Exemplos:

1. Se p é primo então $\mathbb{Z}_p$ só tem anel de valorização $\mathbb{Z}_p$.

2. Seja $\mathbb{Z}_5(X)$ o corpo de frações de $\mathbb{Z}_5[X]$. Como $\overline{\frac{3}{2}} \in \mathbb{Z}_5(X)$ é raiz de $f(x) = \overline{2}X + \overline{2} \in \mathbb{Z}_5[X]$ temos que $\overline{\frac{3}{2}}$ é algébrico sobre $\mathbb{Z}_5$, e então $\mathbb{Z}_5[\overline{\frac{3}{2}}]$ é um corpo que é extensão algébrica de $\mathbb{Z}_5$, e portanto só tem anel de valorização trivial.

3. Seja $\mathbb{Q}$ o corpo dos números racionais. Dado $p \in \mathbb{Z}$ um número primo, considere o conjunto

$$\mathbb{Z}_{(p)} = \{\frac{a}{b}; a,b \in \mathbb{Z} \text{ e } b \notin p\mathbb{Z}\}.$$

O conjunto $\mathbb{Z}_{(p)}$ é um subanel próprio de $\mathbb{Q}$ pois $\frac{1}{p} \notin \mathbb{Z}_{(p)}$. Vamos verificar que $\mathbb{Z}_{(p)}$ é um anel de valorização de $\mathbb{Q}$. Seja $\frac{m}{n}$ uma fração irredutível de $\mathbb{Q}$,

não nula, e suponha que $\frac{m}{n} \notin \mathbb{Z}_{(p)}$. Assim, $p \mid n$, e como a fração é irredutível temos que $p \nmid m$. Portanto, $(\frac{m}{n})^{-1} = \frac{n}{m} \in \mathbb{Z}_{(p)}$.

O anel de valorização $\mathbb{Z}_{(p)}$ do exemplo acima é chamado de anel de valorização p-ádico de $\mathbb{Q}$. O anel $\mathbb{Z}_{(p)}$ é a localização do anel $\mathbb{Z}$ no ideal primo $p\mathbb{Z}$.

Se A é um anel de valorização de $\mathbb{K}$, então a relação de inclusão é uma relação de ordem total no conjunto dos ideais de A, como pode ser visto na Proposição abaixo.

Proposição 3.1.1 *Seja A um anel de valorização de $\mathbb{K}$. Se I e J são ideais de A então $I \subseteq J$ ou $J \subseteq I$.*

Demonstração: Se $I \not\subset J$ então existe $x \in I \backslash J$, $x \neq 0$. Seja $y \in J$. Se $y = 0$ então $y \in I$. Se $y \neq 0$ então $x^{-1}y \in \mathbb{K}^*$. Como A é anel de valorização de $\mathbb{K}$ vem que $x^{-1}y \in A$ ou $xy^{-1} \in A$. No primeiro caso temos $x \in I$ e $x^{-1}y \in A$ que leva a $y \in I$. No segundo caso temos $y \in J$ e $xy^{-1} \in A$ que leva a $x \in J$, o que é contradição. Logo $I \subseteq J$ ou $J \subseteq I$.

■

O resultado anterior fornece outra maneira de verificar que $\mathbb{Z}$ não é anel de valorização de $\mathbb{Q}$ pois $2\mathbb{Z}$ e $3\mathbb{Z}$ são ideais de $\mathbb{Z}$ incomparáveis pela inclusão.

Definição 3.1.2 *O Radical de Jacobson de um anel A é a interseção de todos os ideais maximais de A, e é denotado por $J(A)$.*

Corolário 3.1.1 *Seja A um anel de valorização de $\mathbb{K}$.*

(*a*) *Todo ideal finitamente gerado de A é principal.*

(*b*) *A é um anel local e seu único ideal maximal é $J(A) = A \backslash U(A)$.*

Demonstração:

(*a*) Seja $I = x_1A + \cdots + x_nA$ um ideal finitamente gerado de A. Pela Proposição

3.1.1 temos que $x_iA \subseteq x_jA$ ou $x_jA \subseteq x_iA$ para $i,j = 1,\cdots,n$. Assim, existe $k \in \{1,\cdots,n\}$ tal que $x_kA = I$.

(b) Sejam I e J ideais maximais de A. Então $I \subseteq J$ ou $J \subseteq I$, mas como ambos são maximais temos que $I = J$. Logo A é local e seu único ideal maximal é $J(A)$. Como $J(A)$ é maximal vem que $J(A) \neq A$ e então $J(A) \subseteq A\backslash U(A)$. Seja agora $x \in A\backslash U(A)$. Desde que $x \in A$ e $x^{-1} \notin A$ temos $xA \subsetneq A$. Assim xA é ideal próprio de A e portanto deve estar contido num ideal maximal, isto é, $xA \subseteq J(A)$. Logo $x \in J(A)$.

■

É comum denotar o único ideal maximal do anel de valorização por m_A.

Proposição 3.1.2 *Se A é um anel de valorização de $\mathbb{K}$ então A é integralmente fechado, isto é, $\{x \in \mathbb{K}; x$ é inteiro sobre $A\} = A$.*

Demonstração: Seja $\overline{A} = \{x \in \mathbb{K}; x$ é inteiro sobre $A\}$. É claro que $A \subseteq \overline{A}$ pois dado $a \in A$ temos que a é raiz de $X - a \in A[X]$. Tome agora $x \in \overline{A}$. Podemos assumir $x \neq 0$ pois $x = 0 \in A$. Então $x \in \mathbb{K}$ e $p(x) = 0$ para algum polinômio mônico $p(X) \in A[X]$. Assim podemos escrever $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ com $a_i \in A$. Se $x \in A$ nada temos para fazer. Consideremos $x^{-1} \in A$. Multiplicando a igualdade $x^n = -(a_{n-1}x^{n-1} + \cdots + a_1x + a_0)$ por $x^{-n+1} = (x^{-1})^{n-1} \in A$ temos $x = -(a_{n-1} + a_{n-2}x^{-1} + \cdots + a_1x^{-n+2} + a_0x^{-n+1})$. Como cada parcela do lado direito está em A concluímos que $x \in A$. Portanto $\overline{A} = A$.

■

A próxima Proposição mostra que os anéis de valorização de Dedekind são exatamente os anéis de valorização noetherianos.

Proposição 3.1.3 *Seja A um anel de valorização de $\mathbb{K}$. São equivalentes:*

(i) A é domínio de Dedekind;

(ii) A é anel noetheriano;

(iii) A é domínio principal.

Demonstração:

$(i) \Rightarrow (ii)$ Segue da definição de domínio de Dedekind.

$(ii) \Rightarrow (iii)$ Por hipótese todo ideal de A é finitamente gerado. Segue do Corolário 3.1.1 que todo ideal de A é principal.

$(iii) \Rightarrow (i)$ Para provar que A é domínio de Dedekind precisamos mostrar que A é noetheriano, integralmente fechado e que todo ideal primo não nulo de A é maximal. A Proposição 3.1.2 garante que A é integralmente fechado. Pela hipótese (iii) A é domínio principal. Logo A é domínio noetheriano. Seja I um ideal primo não nulo de A. Então $I = (p)$ e $0 \neq p$ é primo em A. Seja $J = (q)$ um ideal maximal contendo I. Assim, $(p) \subseteq (q)$ e daí $p = qt$ para algum $t \in A$. Como p é primo temos que $p \mid q$ ou $p \mid t$. Se $p \mid t$ então $t = pu$, para algum $u \in A$. Segue que $p = qt = qpu$, e como A é domínio temos $qu = 1$ implicando em $(q) = A$. Absurdo pois (q) é ideal maximal. Portanto devemos ter $p \mid q$, e assim $(q) \subseteq (p)$. Logo, $(p) = (q)$ é ideal maximal.

■

Vamos destacar ainda dois importantes resultados sobre anéis de valorização. O primeiro deles, conhecido como Teorema da Correspondência, relaciona ideais primos do anel de valorização A do corpo $\mathbb{K}$, com os sobreanéis de A em $\mathbb{K}$. O segundo resultado é o Teorema da Extensão que possibilita obter um anel de valorização V para o corpo $L \supseteq \mathbb{K}$ tal que $V \cap \mathbb{K} = A$.

Sejam A um anel de valorização do corpo $\mathbb{K}$, e B um sobreanel de A em $\mathbb{K}$, isto é, $A \subseteq B \subseteq \mathbb{K}$. É claro que B é um anel de valorização de $\mathbb{K}$, e então pelo Corolário 3.1.1, $J(B) = B \backslash U(B)$ é o único ideal maximal de B.

Afirmação: $J(B) \subseteq J(A)$.

De fato, se $x \in J(B) = B \backslash U(B)$ então $x \in B$ e $x^{-1} \notin B$. Como $A \subseteq B$ vemos que $x^{-1} \notin A$, e portanto $x \in A$. Logo $x \in A \backslash U(A) = J(A)$.

Usando as notações:

$$\beta = \{B \subseteq \mathbb{K}; B \text{ é anel e } A \subseteq B\}$$

$$\wp = \{P \subseteq A; P \text{ é ideal primo}\},$$

obtivemos uma aplicação

$$\psi : \beta \to \wp$$

dada por $\psi(B) = J(B)$, que reverte a inclusão. Lembre que $J(B)$ é ideal primo por ser maximal.

Por outro lado, dado $P \in \wp$, consideremos o conjunto $S = A - P$. Desde que P é ideal primo é fácil ver que:

(a) $1 \in S$;

(b) $0 \notin S$;

(c) $x, y \in S \Rightarrow xy \in S$.

Estas condições asseguram que S é um sistema multiplicativo e que $A_P = \{\frac{a}{b}; a, b \in A, b \notin P\}$ é um sobreanel de A em $\mathbb{K}$. Temos então a aplicação

$$\varphi : \wp \to \beta$$

dada por $\varphi(p) = A_p$.

Teorema 3.1.1 (Teorema da Correspondência) *A aplicação $\psi : \beta \to \wp$ dada por $\psi(B) = J(B)$ é bijetora e $\psi^{-1} = \varphi$.*

Demonstração: Precisamos provar que $A_{J(B)} = B$ e $J(A_P) = P$ para todo anel B tal que $A \subseteq B \subseteq \mathbb{K}$, e para todo ideal primo P de A. Mas $A \subseteq A_{J(B)} = \{\frac{a}{b}; a, b \in A \text{ e } b \notin J(B)\}$ e $A \subseteq B$. Assim $b \in B$ e $b \notin J(B) = B \backslash U(B)$,

que leva a $b^{-1} \in B$. Logo, $A_{J(B)} \subseteq B$. Seja agora $x \in B$, e consideremos $x \neq 0$. Se $x \in A$ então $x \in A_{J(B)}$. Se $x^{-1} \in A$ então $x^{-1} \in B$. Como $J(B)$ é ideal próprio e $x \in B$ vem que $x^{-1} \notin J(B)$. Escrevemos então $x = \frac{1}{x^{-1}} \in A_{J(B)}$ provando que $B \subseteq A_{J(B)}$. Para ver que $J(A_P) = P$ começamos observando que A_P é anel de valorização e portanto $J(A_P) = A_P \backslash U(A_P)$. Desde que $U(A_P) = \{\frac{a}{b}; a, b \in A \text{ e } a, b \notin P\}$ vem que $J(A_P) = \{\frac{a}{b}; a, b \in A, b \notin P \text{ e } a \in P\}$. Escrevendo $p \in P$ como $p = \frac{p}{1}$ temos que $p \in J(A_P)$ e daí $P \subseteq J(A_P)$. Por outro lado, a inclusão $A \subseteq A_P$ garante que $J(A_P) \subseteq J(A) \subseteq A$. Dado $a \cdot b^{-1} \in J(A_P)$ temos que $a, b \in A$, $b \notin P$, $a \in P$ e também $a \cdot b^{-1} = d \in A$. Assim $bd = a \in P$, e como P é ideal primo e $b \notin P$ temos $d \in P$, isto é, $a \cdot b^{-1} \in P$. Logo, $J(A_P) \subseteq P$.

■

Sejam $\mathbb{K}$ e L corpos tais que $\mathbb{K} \subseteq L$. Se V é um anel de valorização de L, então é claro que $A = V \cap \mathbb{K}$ é um anel de valorização de $\mathbb{K}$. O Teorema da Extensão garante que todo anel de valorização de $\mathbb{K}$ pode ser obtido desta forma.

Teorema 3.1.2 (Teorema da Extensão) *Seja $\mathbb{K} \subseteq L$ uma extensão de corpos. Se A é um anel de valorização de $\mathbb{K}$ então existe um anel de valorização V de L tal que $A = \mathbb{K} \cap V$.*

Demonstração: ([7], Theorem 13.2, pg 94).

■

3.2 Valorizações de Krull

As valorizações de Krull aparecem como uma generalização da definição de valorização exponencial vista na seção 2.4. Faremos um estudo sobre valorizações de Krull, relacionando tais valorizações com os anéis de valorização.

Seja $(G, +)$ um grupo abeliano totalmente ordenado pela relação $\leq$. Denotemos a união do símbolo ∞ ao grupo G por $G \cup \{\infty\}$, e consideremos as convenções:

- $g + \infty = \infty + g = \infty + \infty = \infty$, para todo $g \in G$;
- $g < \infty$, para todo $g \in G$;
- $g_1 \leq g_2 \Rightarrow g_1 + h \leq g_2 + h$, para todos $g_1, g_2, h \in G$.

Definição 3.2.1 *Seja $\mathbb{K}$ um corpo. Uma função $v : \mathbb{K} \to G \cup \{\infty\}$ é uma valorização de Krull quando:*

(VE_1) $v(x) = \infty \Leftrightarrow x = 0$;

(VE_2) $v(xy) = v(x) + v(y)$, *para todos* $x, y \in \mathbb{K}$;

(VE_3) $v(x + y) \geq min\{v(x), v(y)\}$, *para todos* $x, y \in \mathbb{K}$.

Note que sempre podemos considerar v como sendo uma função sobrejetora. De fato, a condição (VE_2) assegura que v é um homomorfismo entre os grupos $(\mathbb{K}^*, \cdot)$ e $(G, +)$. Então, se for necessário podemos trocar G pelo grupo $v(\mathbb{K}^*)$.

O grupo G é chamado de grupo de valores de v. Daqui em diante, como é comum, fazeremos referência as valorizações de Krull apenas como valorizações.

Nosso objetivo é relacionar as valorizações de um corpo com os anéis de valorização deste corpo. Começamos com um Lema sobre propriedades de uma valorização.

Lema 3.2.1 *Seja v uma valorização do corpo $\mathbb{K}$. Então:*

(a) $v(1) = v(-1) = 0$;

(b) $v(-x) = v(x)$, *para todo* $x \in \mathbb{K}$;

(c) $v(x^{-1}) = -v(x)$, *para todo* $x \in \mathbb{K}^*$.

Demonstração:

(a) Por (VE_2) temos claramente que $v(1) = 0$. Daí escrevemos $0 = v(1) =$

$v((-1).(-1)) = v(-1) + v(-1)$. Desde que o grupo de valores de v é totalmente ordenado isso implica em $v(-1) = 0$. De fato, supondo que $v(-1) > 0$ vem que $v(-1) + v(-1) > v(-1) > 0$ implicando em $v(1) > 0$. Contradição. Analogamente não podemos ter $v(-1) < 0$.

(b) $v(-x) = v(-1 \cdot x) = v(-1) + v(x) = 0 + v(x) = v(x)$.

(c) $0 = v(1) = v(x \cdot x^{-1}) = v(x) + v(x^{-1}) \Rightarrow v(x^{-1}) = -v(x)$.

■

Proposição 3.2.1 *Seja v uma valorização do corpo $\mathbb{K}$.*

(a) $A_v = \{x \in \mathbb{K}; v(x) \geq 0\}$ *é um anel de valorização de* $\mathbb{K}$;

(b) $J_v = \{x \in \mathbb{K}; v(x) > 0\}$ *é o único ideal maximal de* A_v;

(c) $J(A_v) = J_v = \{x \in A_v; x = 0$ *ou* $x^{-1} \notin A_v\}$

Demonstração:

(a) Desde que $v(0) = \infty$ e $v(1) = 0$, é claro que $0, 1 \in A_v$. Dados $x, y \in A_v$ também temos $v(xy) = v(x) + v(y) \geq v(y) \geq 0$, e assim $xy \in A_v$. Além disso, $v(x - y) = v(x+(-y)) \geq min\{v(x), v(-y)\} = min\{v(x), v(y)\} \geq 0$, isto é, $x-y \in A_v$. Portanto A_v é um subanel de $\mathbb{K}$. Para ver que A_v é um anel de valorização de $\mathbb{K}$ tomamos $x \in \mathbb{K}$, $x \neq 0$. Como $v(x^{-1}) = -v(x)$ vemos que $v(x) \geq 0$ ou $v(x^{-1}) \geq 0$, e então $x \in A_v$ ou $x^{-1} \in A_v$.

(b) Para mostrar que J_v é um ideal de A_v, tomamos $x \in J_v$ e $y \in A_v$. Assim, $v(x) > 0$ e $v(y) \geq 0$. Agora $v(xy) = v(x) + v(y) > 0$, e então $xy \in J_v$. Logo J_v é ideal de A_v. Desde que A_v é um anel de valorização de $\mathbb{K}$, sabemos da seção anterior que seu único ideal maximal é dado por $A_v \backslash U(A_v)$. Portanto vamos provar que $J_v = A_v \backslash U(A_v)$. Como $1 \notin J_v$ temos que J_v é um ideal próprio de A_v, e então deve estar contido num ideal maximal. Sendo $A_v \backslash U(A_v)$ o único ideal maximal de A_v segue que $J_v \subseteq A_v \backslash U(A_v)$. Seja agora $x \in A_v \backslash U(A_v)$. Então $v(x) \geq 0$ e $v(x^{-1}) < 0$ o que implica em $v(x) \geq 0$ e $-v(x) < 0$. Portanto $v(x) > 0$ e $x \in J_v$.

(c) Desde que $J(A_v)$ é a interseção de todos os ideais maximais de A_v, temos pelo

item (b) que $J(A_v) = J_v$. Se $x \in J_v$ e $x \neq 0$ então $v(x^{-1}) = -v(x) < 0$. Isso implica em $x^{-1} \notin A_v$ e daí $J_v \subseteq \{x \in A_v; x = 0 \text{ ou } x^{-1} \notin A_v\}$. Por outro lado, se $x \in A_v$, $x \neq 0$ e $x^{-1} \notin A_v$ temos que $-v(x) = v(x^{-1}) < 0$ que leva a $x \in J_v$.

■

Com a notação da Proposição anterior temos a seguinte definição.

Definição 3.2.2 *Duas valorizações v e v' de $\mathbb{K}$ são equivalentes quando $A_v = A_{v'}$.*

Denotanto por $[v]$ a classe de equivalência da valorização v, temos uma aplicação

$$\psi : \{[v]; v \text{ é valorização de } \mathbb{K}\} \to \{A; A \text{ é anel de valorização de } \mathbb{K}\}$$

$$[v] \mapsto A_v$$

Veremos agora como associar a cada anel de valorização do corpo $\mathbb{K}$, uma valorização de $\mathbb{K}$.

Seja A um anel de valorização de $\mathbb{K}$. No conjunto

$$G = \{xA; x \in K^*\}$$

defina a operação

$$xA + yA = (xy)A.$$

É fácil ver que G é um grupo abeliano cujo elemento neutro é $A = 1 \cdot A$.

Para que G seja o grupo de valores de alguma valorização de $\mathbb{K}$, precisamos ter uma relação de ordem total em G. Fazemos isso escrevendo $xA \leq yA$ quando $yA \subseteq xA$. Note que isso de fato define uma relação de ordem total em G, pois dados $x, y \in \mathbb{K}^*$ temos $xy^{-1} \in \mathbb{K}^*$. Daí $xy^{-1} \in A$ ou $x^{-1}y \in A$. Se $xy^{-1} \in A$

então $xy^{-1} \cdot A \subseteq A$ implicando em $xA \subseteq yA$. Analogamente $x^{-1}y \in A$ implica em $yA \subseteq xA$.

Com as convenções feitas no início desta seção para unir G ao símbolo ∞, definimos

$$v : \mathbb{K} \to G \cup \{\infty\}$$

$$0 \mapsto \infty$$

$$x \mapsto xA, x \neq 0.$$

Proposição 3.2.2 *Com as notações estabelecidas acima temos:*

(a) *v é uma valorização de $\mathbb{K}$;*

(b) *$A_v = A$;*

(c) *Existe uma correspondência biunívoca entre anéis de valorização de $\mathbb{K}$ e classes de valorização de $\mathbb{K}$.*

Demonstração:

(a) A condição (VE_1) é evidente. Para verificar (VE_2) tomamos $x, y \in \mathbb{K}$, e observamos inicialmente que se $x = 0$ ou $y = 0$ a condição é satisfeita. Assim podemos assumir $x \neq 0$ e $y \neq 0$, isto é, $v(x) = xA$ e $v(y) = yA$. Pela definição da operação em G temos $v(xy) = (xy)A = xA + yA = v(x) + v(y)$, e portanto vale (VE_2). Novamente tomamos $x, y \in \mathbb{K}$ e observamos que (VE_3) é evidente quando $x+y = 0$. Quando $x + y \neq 0$ vem que $v(x + y) = (x + y)A \subseteq xA + yA$. Como G é totalmente ordenado devemos ter $xA \subseteq yA$ ou $yA \subseteq xA$, implicando em $xA + yA \subseteq yA$ ou $xA + yA \subseteq xA$. Podemos escrever então $v(x + y) \subseteq zA$, onde zA é o maior, na relação de inclusão, entre xA e yA. Assim, $zA = min\{xA, yA\}$ segundo a relação $\leq$. Portanto, $v(x + y) \geq zA = min\{xA, yA\} = min\{v(x), v(y)\}$.

(b) Como o elemento neutro de G é A, vemos que $A_v = \{x \in \mathbb{K}; v(x) \geq A\} = \{0\} \cup \{x \in \mathbb{K}^*; xA \subseteq A\} = A$.

(c) Temos definidas as aplicações

$$\psi : \{[v]; v \text{ é valorização de } \mathbb{K}\} \longrightarrow \{A; A \text{ é anel de valorização de } \mathbb{K}\}$$

$$[v] \mapsto Av$$

$$\varphi\{A; A \text{ é anel de valorização de } \mathbb{K}\} \longrightarrow \{[v]; v \text{ é valorização de } \mathbb{K}\}$$

$$A \mapsto [v]$$

com $A_v = A$, pelo item (b).

- $\psi(\varphi(A)) = \psi([v])$, onde v é tal que $A_v = A$. Assim $\psi(\varphi(A)) = A_v = A$.
- $\varphi(\psi[v]) = \varphi(A_v) = [w]$ onde $A_w = A_v$. Daí $[w] = [v]$ e portanto $\varphi(\psi([v])) = [v]$.

■

Exemplos:

1. Todo corpo $\mathbb{K}$ possui uma valorização, chamada de valorização trivial, onde tomamos $G = \{0\}$ e definimos

$$v : \mathbb{K} \longrightarrow G \cup \{\infty\}$$

$$0 \mapsto \infty$$

$$x \mapsto 0; x \neq 0.$$

Note que a valorização trivial está associada ao anel de valorização trivial, isto é, $A_v = \mathbb{K}$.

2. Para cada número primo p podemos definir a valorização p-ádica de $\mathbb{Q}$. Para isso observamos que dado $\frac{a}{b} \in \mathbb{Q}$ podemos escrever $\frac{a}{b} = p^n \cdot \frac{r}{s}$, onde $n \in \mathbb{Z}$ e r, s são primos relativos com p. Definimos

$$v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

$$0 \mapsto \infty$$

$$\frac{a}{b} = p^n \cdot \frac{r}{s} \mapsto n.$$

Não é difícil verificar que v_p é uma valorização de $\mathbb{Q}$. Além disso, dado $\frac{a}{b} \in \mathbb{Q}$ temos que:

$$\frac{a}{b} \in A_v \Leftrightarrow v_p(\frac{a}{b}) \geq 0 \Leftrightarrow p \nmid b \Leftrightarrow \frac{a}{b} \in \mathbb{Z}(p).$$

Portanto, $A_v = \mathbb{Z}(p)$, isto é, a valorização p-ádica está associada ao anel de valorização p-ádico de $\mathbb{Q}$.

3.3 Teorema da Aproximação para Anéis de Valorização

Daqui em diante nosso principal objetivo passa a ser demonstrar o Teorema da Aproximação para anéis de valorização. Além disso, definiremos anel de Prüfer e, a partir dessa definição e de algumas propriedades, demonstraremos a versão fraca do Teorema da Aproximação para anéis de valorização. Para demonstrarmos a versão forte de tal Teorema, precisamos ainda definir anéis de valorização independentes. Vale a pena ressaltar que em ambas as versões do Teorema da Aproximação utilizamos o Teorema Chinês de Restos nas suas demonstrações.

Definição 3.3.1 *Seja R um anel e M um subconjunto de R. Dizemos que M é um sistema multiplicativo de R quando*

(*a*) $1 \in M$;

(*b*) $0 \notin M$;

(c) $m, m' \in M \Rightarrow m \cdot m' \in M$.

Exemplos:

1. O conjunto dos elementos inversíveis do anel R, isto é, $M = U(R)$, é um sistema multiplicativo para R.
2. Se R é um domínio então $M = R^*$ é um sistema multiplicativo para R.
3. Se P é um ideal primo de R então $M = R - P$ é um sistema multiplicativo para R.

Se R é um subanel do corpo $\mathbb{K}$ e M é um sistema multiplicativo para R podemos definir o conjunto

$$R_M = \{r \cdot m^{-1}; r \in R \text{ e } m \in M\} \subseteq \mathbb{K}.$$

É claro que $0, 1 \in R_M$ e que R_M é fechado por produto. Além disso, dados $rm^{-1}, sn^{-1} \in R_M$ temos que $rm^{-1} - sn^{-1} = (rn - sm)(mn)^{-1}$. Portanto, R_M é um subanel de $\mathbb{K}$ que contém R.

Definição 3.3.2 *O anel R_M é chamado de anel de frações de R, segundo o sistema multiplicativo M.*

Definição 3.3.3 *Sejam R um subanel do corpo $\mathbb{K}$ e A um anel de valorização de $\mathbb{K}$. Dizemos que A é essencial para R quando $A = R_M$, para algum sistema multiplicativo M de R.*

Usaremos as notações:

$\epsilon(R)$ para o conjunto dos anéis de valorização de $\mathbb{K}$ que são essenciais para R.

$\beta(R)$ para o conjunto dos anéis de valorização de $\mathbb{K}$ que contém R.

Como $R \subseteq R_M$, para todo sistema multiplicativo M, temos que $\epsilon(R) \subseteq \beta(R)$.

Definição 3.3.4 *Um subanel R do corpo $\mathbb{K}$ é chamado de Anel de Prüfer de $\mathbb{K}$ quando $\epsilon(R) = \beta(R)$.*

Para cada anel de valorização A do corpo $\mathbb{K}$ temos o homomorfismo projeção canônica

$$\varphi_A : A \to \frac{A}{m_A}$$

$$a \mapsto a + m_A$$

onde m_A é o único ideal maximal de A.

Proposição 3.3.1 *Seja R um subanel do corpo $\mathbb{K}$.*

(a) Se $A \in \beta(R)$ então $\varphi_A(R) \subseteq \frac{A}{m_A}$;

(b) Se $A \in \beta(R)$ e $\varphi_A(R) = \frac{A}{m_A}$ então $m_A \cap R$ é um ideal maximal de R.

(c) Se $A \in \epsilon(R)$ são equivalentes:

(i) $\varphi_A(R) = \frac{A}{m_A}$

(ii) $m_A \cap R$ é ideal maximal de R.

Demonstração:

(a) É óbvio pois $R \subseteq A$.

(b) Por hipótese $R \subseteq A$ e $\varphi_A \mid_R$: $R \to \frac{A}{m_A}$ é um homomorfismo sobrejetor de anéis. É fácil ver que $Ker(\varphi_A \mid_R) = R \cap m_A$, e então $\frac{R}{m_A \cap R}$ é isomorfo a $\frac{A}{m_A}$. Desde que $\frac{A}{m_A}$ é corpo temos que $\frac{R}{m_A \cap R}$ também é corpo, e portanto $m_A \cap R$ é ideal maximal de R.

(c) $(i) \Rightarrow (ii)$ Segue de (b) pelo fato de $\epsilon(R) \subseteq \beta(R)$.

$(ii) \Rightarrow (i)$ Como $m_A \cap R$ é ideal maximal de R, temos pelo exemplo 3, que $S = R - (m_A \cap R)$ é um sistema multiplicativo de R. Por outro lado, desde que $A \in \epsilon(R)$, existe um sistema multiplicativo M de R tal que $A = R_M$. Suponha

que exista $x \in M \cap m_A$. De $x \in M$ vem que $x^{-1} = 1 \cdot x^{-1} \in R_M = A$, mas como $x \in m_A$ isso leva a $1 = x \cdot x^{-1} \in m_A$. Contradição. Logo $M \cap m_A = \emptyset$ e daí $M \cap (m_A \cap R) = \emptyset$ e portanto $M \subseteq R - (m_A \cap R) = S$. Agora concluímos que $A \subseteq R_S$ pois $A = R_M \subseteq R_S$. Se $rm^{-1} \in R_S$ temos $r \in R \subseteq A$ e $m \in S = R - (m_A \cap R)$, isto é, $r \in A$, $m \in A$ e $m \notin m_A$, que leva a $r \in A$ e $m^{-1} \in A$. Portanto $rm^{-1} \in A$ e assim $R_S \subseteq A$. Verificamos então que $A = R_S = R_M$. Para provar que $\varphi_A(R) = \frac{A}{m_A}$ basta mostrar que $\frac{A}{m_A} \subseteq \varphi_A(R)$. Seja $\overline{a} = a + m_A \in \frac{A}{m_A}$. Como $a \in A = R_S$ vem que $a = uv^{-1}$, onde $u \in R$ e $v \in S$, isto é, $u, v \in R$ e $v \notin m_A \cap R$. Por hipótese $m_A \cap R$ é ideal maximal de R, e então $(m_A \cap R) + vR = R$. Obtemos então $r \in R$ e $\alpha \in m_A \cap R$ tais que $1 = \alpha + vr$. Segue que $vr = 1 - \alpha$, dai $r = v^{-1}(1 - \alpha)$ e $ur = uv^{-1}(1 - \alpha) = a(1 - \alpha) = a - a\alpha$. Finalmente, $ur \in R$ e $\varphi(ur) = \overline{a - a\alpha} = \overline{a} - \overline{a\alpha} = \overline{a}$ pois $\alpha \in m_A$. Isso prova que $\varphi_A(R) = \frac{A}{m_A}$.

■

O Teorema abaixo é um dos resultados importantes, que usaremos na demonstração do Teorema da Aproximação para anéis de valorização. Sua demonstração pode ser vista em ([7], Theorem 11.12).

Teorema 3.3.1 *Sejam $A_1, \cdots, A_k$ anéis de valorizações do corpo $\mathbb{K}$, dois a dois incomparáveis pela relação de inclusão. Então $R = A_1 \cap \cdots \cap A_k$ é um anel de Prüfer de $\mathbb{K}$, e seus ideais maximais distintos são exatamente $m_{A_1} \cap R, \cdots, m_{A_k} \cap R$. Além disso, existe uma correspondência biunívoca entre $\beta(R) = \epsilon(R)$ e os ideais primos de R dada por $A \mapsto m_A \cap R$, $P \mapsto R_{(R-P)}$.*

Corolário 3.3.1 *Sejam $A_1, \cdots, A_k$ anéis de valorizações do corpo $\mathbb{K}$, dois a dois incomparáveis pela relação de inclusão, e $R = A_1 \cap \cdots \cap A_k$. Então para cada $i \in \{1, \cdots, k\}$ temos $\varphi_{A_i}(R) = \frac{A_i}{m_{A_i}}$.*

Demonstração: Para cada $i \in \{1, \cdots, k\}$ temos $R \subseteq A_i$, isto é, $A_i \in \beta(R)$. Pelo Teorema 3.3.1, R é um anel de Prüfer de $\mathbb{K}$, e então $A_i \in \beta(R) = \epsilon(R)$. Também pelo Teorema 3.3.1, vemos que $m_{A_i} \cap R$ é ideal maximal de R. Agora usamos a

Proposição 3.3.1, item (c) para obter que $\varphi_{A_i}(R) = \frac{A_i}{\eta_{A_i}}$.

■

Provaremos a seguir o resultado conhecido como versão fraca do Teorema da Aproximação para anéis de valorização.

Teorema 3.3.2 *Sejam $A_1, \cdots, A_k$ anéis de valorização do corpo $\mathbb{K}$, dois a dois incomparáveis pela relação de inclusão, e $R = A_1 \cap \cdots \cap A_k$. Então para cada $(a_1, \cdots, a_k) \in A_1 \times \cdots \times A_k$ existe $d \in R$ tal que $(d-a_1, \cdots, d-a_k) \in \eta_{A_1} \times \cdots \times \eta_{A_k}$.*

Demonstração: Para cada $i \in \{1, \cdots, k\}$ temos o homomorfismo $\varphi_{A_i} : A_i \to \frac{A_i}{\eta_{A_i}}$, e pelo Corolário 3.3.1 vem que $\varphi_{A_i}(R) = \frac{A_i}{\eta_{A_i}}$. Assim para $a_i \in A_i$ existe $d_i \in R$ tal que $\varphi(d_i) = \overline{a_i}$, isto é, $d_i + \eta_{A_i} = a_i + \eta_{A_i}$ e portanto $d_i - a_i \in \eta_{A_i}$. Do Teorema 3.3.1 tiramos que $\eta_{A_1} \cap R, \cdots, \eta_{A_k} \cap R$ são ideais maximais distintos de R, e portanto $\eta_{A_1} \cap R, \cdots, \eta_{A_k} \cap R$ são ideais dois a dois comaximais de R. Aplicando o Teorema Chinês de Restos (Teorema 1.1.1) aos elementos $d_1, \cdots, d_k \in R$ e aos ideais $\eta_{A_1} \cap R, \cdots, \eta_{A_k} \cap R$, obtemos $d \in R$ tal que $d - d_i \in \eta_{A_i} \cap R$. Logo $d - a_i = (d - d_i) + (d_i - a_i) \in \eta_{A_i}$.

■

Para provar a versão forte do Teorema da Aproximação para anéis de valorização precisamos nos restringir aos anéis de valorização independentes.

Definição 3.3.5 *Sejam A_1 e A_2 anéis de valorização do corpo $\mathbb{K}$. Dizemos que A_1 e A_2 são independentes quando o único anel de valorização de $\mathbb{K}$ que contém A_1 e A_2 é o próprio corpo $\mathbb{K}$.*

Note que o fato de A_1 e A_2 serem independentes não implica em A_1 e A_2 serem incomparáveis, pois podemos ter $A_1 = \mathbb{K}$ e $A_2 \subsetneq \mathbb{K}$. No entanto, se A_1 e A_2 são diferentes de $\mathbb{K}$ então a independência implica que A_1 e A_2 são incomparáveis.

Se A_1 e A_2 são anéis de valorização do corpo $\mathbb{K}$, definimos

$$A_1 \cdot A_2 = \{\sum_{i=1}^{n} a_i b_i; a_i \in A_1 \text{ e } b_i \in A_2\}.$$

É fácil ver que $A_1 \cdot A_2$ é um subanel de $\mathbb{K}$ que contém A_1 e A_2. Logo, $A_1 \cdot A_2$ é um anel de valorização de $\mathbb{K}$. Além disso $A_1 \cdot A_2$ é o menor subanel de $\mathbb{K}$ que contém A_1 e A_2.

Proposição 3.3.2 *Sejam A_1 e A_2 anéis de valorização de $\mathbb{K}$. São equivalentes:*

(i) *A_1 e A_2 são independentes;*

(ii) $A_1 \cdot A_2 = \mathbb{K}$;

(iii) $m_{A_1 \cdot A_2} = (0)$.

Demonstração:
(i) $\Leftrightarrow$ *(ii)* Assumindo que A_1 e A_2 são independentes é claro que $A_1 \cdot A_2 = \mathbb{K}$ pois $A_1, A_2 \subseteq A_1 \cdot A_2$ e $A_1 \cdot A_2$ é anel de valorização de $\mathbb{K}$. Reciprocamente, se $A_1 \cdot A_2 = \mathbb{K}$ temos que o menor subanel de $\mathbb{K}$ que contém A_1 e A_2 é $\mathbb{K}$. Logo, A_1 e A_2 são independentes.
(ii) $\Leftrightarrow$ *(iii)* Se $A_1 \cdot A_2 = \mathbb{K}$ então $A_1 \cdot A_2$ é corpo e seu único ideal maximal é $m_{A_1 \cdot A_2} = (0)$. Reciprocamente, se (0) é o único ideal maximal de $A_1 \cdot A_2$ então $A_1 \cdot A_2 = \mathbb{K}$ pelo Teorema da Correspondência (Teorema 3.1.1).

■

Lembramos que se I é um ideal do anel R, $I \neq R$, então o radical de I é dado por

$$\sqrt{I} = \{x \in R; x^n \in I \text{ para algum } n \in \mathbb{N}\}.$$

Claramente $\sqrt{I}$ é um ideal próprio de R pois $1 \notin \sqrt{I}$. Também $I \subseteq \sqrt{I}$, e vale a igualdade quando I é ideal primo de R.

Lema 3.3.1 *Seja A um anel de valorização de $\mathbb{K}$. Se I é um ideal próprio de A então $\sqrt{I}$ é um ideal primo de A.*

Demonstração: Desde que $\sqrt{I}$ é um ideal próprio de A, basta provar que $a \in \sqrt{I}$ ou $b \in \sqrt{I}$ quando $a, b \in A$ e $ab \in \sqrt{I}$. Seja $n \in \mathbb{N}$ tal que $(ab)^n \in I$. Pela Proposição 3.1.1 devemos ter $A \cdot a \subseteq A \cdot b$ ou $A \cdot b \subseteq A \cdot a$. Se $A \cdot b \subseteq A \cdot a$ então $b^{2n} \in Ab^n \cdot Ab^n \subseteq Ab^n \cdot Aa^n \subseteq Aa^n b^n \in I$ implicando em $b \in \sqrt{I}$. Analogamente temos $a \in \sqrt{I}$ quando $Aa \subseteq Ab$.

■

Note que se R é subanel de A e I é um ideal próprio de A então $\sqrt{I} \cap R = \sqrt{I \cap R}$. De fato, como $I \cap R$ é ideal de R temos

$$\sqrt{I} \cap R = \{x \in A; x^n \in I \text{ para algum } n \in \mathbb{N}\} \cap R =$$

$$= \{x \in R; x^n \in I \text{ para algum } n \in \mathbb{N}\} =$$

$$= \{x \in R; x^n \in I \cap R \text{ para algum } n \in \mathbb{N}\} = \sqrt{I \cap R}.$$

Proposição 3.3.3 *Sejam $A_1, \cdots, A_k$ anéis de valorização de $\mathbb{K}$, dois a dois independentes, $R = A_1 \cap \cdots \cap A_k$ e $I_i \neq 0$ um ideal próprio de A_i, para $i \in \{1, \cdots, k\}$. Então $I_1 \cap R, \cdots, I_k \cap R$ são ideais dois a dois comaximais de R.*

Demonstração: Podemos assumir $k \geq 2$ e que $A_i \neq \mathbb{K}$. Assim, $A_1 \cdots, A_k$ também são incomparáveis. Sejam $B_i = m_{A_i} \cap R$ e $C_i = I_i \cap R$. É claro que $C_i \subseteq B_i$ pois $I_i \subseteq m_{A_i}$. Pelo Teorema 3.3.1 temos que $A_i \in \beta(R) = \epsilon(R)$ e então $A_i = R_{S_i}$, onde S_i é o sistema multiplicativo $R - B_i$. Assim I_i é ideal de R_{S_i} e deve estar contido no seu único ideal maximal, isto é, $I_i \subseteq B_i \cdot R_{S_i} = (m_{A_i} \cap R) \cdot R_{S_i} \subseteq (I_i \cap R) \cdot A_i \subseteq I_i$. Como $I_i \neq 0$ e $I_i = (I_i \cap R) \cdot A_i$ vem que $C_i = I_i \cap R \neq 0$. Suponha que $C_1, \cdots, C_k$ não são ideais dois a dois comaximais. Então existem $i, j \in \{1, \cdots, k\}$, $i \neq j$, tais que $C_i + C_j$ está contido em algum ideal maximal m de R. Pelo Teorema 3.3.1 concluímos que $m = B_h$ para algum $h \in \{1, \cdots, k\}$. Reordenando

convenientemente os conjuntos $\{C_1, \cdots, C_k\}$ e $\{B_1, \cdots, B_k\}$ podemos assumir que $C_1 \subseteq B_2$. O Lema 3.3.1 diz que $\sqrt{I_1}$ é um ideal primo de A_1 e então $\sqrt{C_1} = \sqrt{I_1} \cap R$ é um ideal primo de R. Como $C_1 \subseteq B_2$ e B_2 é ideal primo de R temos $\sqrt{C_1} \subseteq \sqrt{B_2} = B_2$, e claramente $\sqrt{C_1} \subseteq \sqrt{B_1} = B_1$ pois B_1 é ideal primo de R. Desde que $\sqrt{C_1}$, B_1 e B_2 são ideais primos de R, $\sqrt{C_1} \subseteq B_1$ e $\sqrt{C_1} \subseteq B_2$ temos os sistemas multiplicativos $S_1 = (R - B_1) \subseteq (R - \sqrt{C_1})$ e $S_2 = (R - B_2) \subseteq (R - \sqrt{C_1})$, que levam a $A_1 = R_{S_1} \subseteq R_{(R-\sqrt{C_1})}$ e $A_2 = R_{S_2} \subseteq R_{(R-\sqrt{C_1})}$. Chamando $R_B = R_{(R-\sqrt{C_1})}$ vemos que $A_1, A_2 \subseteq R_B$, e como A_1 e A_2 são independentes segue que $R_B = \mathbb{K}$. Assim o único ideal maximal de R_B é $\sqrt{C_1} \cdot R_B = 0$, implicando em $\sqrt{C_1} = 0$, donde $C_1 = 0$. Isso leva a contradição.

■

Lema 3.3.2 *Sejam A um anel de valorização próprio de $\mathbb{K}$ com valorização correspondente $v : \mathbb{K} \to G \cup \{\infty\}$, $c \in A$, $c \neq 0$ e $x \in G$. Então*
$I = \{a \in m_A; v(a) > v(c) + x\}$ é um ideal próprio de A e $I \neq 0$.

Demonstração: É claro que se a e b estão em I então $v(a+b) \geq min\{v(a), v(b)\} > v(c) + x$, isto é, $a + b \in I$. Se $a \in I$ e $\alpha \in A$ então $v(\alpha) \geq 0$ implicando em $v(a\alpha) = v(a) + v(\alpha) \geq v(a) > v(c) + x$. Portanto, I é um ideal de A e $I \neq A$ pois $I \subseteq m_A \subsetneq A$. Para ver que $I \neq 0$ dividiremos em dois casos: $x \leq 0$ e $x > 0$. Consideremos inicialmente $x > 0$. Como v pode ser tomada sobrejetora, existe $\tilde{a} \in \mathbb{K}^*$ tal que $v(\tilde{a}) = x > 0$, e então $\tilde{a} \in m_A$. Tomando $a = \tilde{a} \cdot \tilde{a} \cdot c \in m_A$ temos $v(a) = v(\tilde{a}) + v(\tilde{a}) + v(c) = v(c) + x + v(\tilde{a}) > v(c) + x$, garantindo que $0 \neq a \in I$. Para o caso $x \leq 0$, tomamos $u \in m_A$, $u \neq 0$. Note que este elemento existe pois $A \neq \mathbb{K}$ implica em $m_A \neq 0$. Escolhendo $a = u \cdot c \in m_A$, $a \neq 0$, temos $v(a) = v(u) + v(c) > v(c) \geq v(c) + x$, pois $v(u) > 0$, já que $u \in m_A$. Portanto $0 \neq a \in I$.

■

Demonstraremos agora o principal resultado deste capítulo, conhecido como Teorema da Aproximação para anéis de valorização, que é uma versão do Teorema

da Aproximação para valorizações exponenciais visto no capítulo 2.

Teorema 3.3.3 (Teorema da Aproximação) *Sejam* $A_1, \cdots, A_k$ *anéis de valorização de* $\mathbb{K}$*, dois a dois independentes, e* $v_i : \mathbb{K} \to G_i \cup \{\infty\}$ *as valorizações correspondentes a* A_i*,* $i \in \{1, \cdots, k\}$*. Dados* $(x_1, \cdots, x_k) \in \mathbb{K} \times \cdots \times \mathbb{K}$ *e* $(\gamma_1, \cdots, \gamma_k) \in G_1 \times \cdots \times G_k$*, existe uma infinidade de elementos* $x \in \mathbb{K}$ *tais que* $v_i(x - x_i) = \gamma_i$*.*

Demonstração: Podemos considerar que $A_i \neq \mathbb{K}$, pois $i \in \{1, \cdots, k\}$. De fato, se $A_i = \mathbb{K}$ então a valorização correspondente é a valorização trivial $v_i : \mathbb{K} \to \{0\} \cup \{\infty\}$, que permite tomarmos qualquer $x \in \mathbb{K}$, $x \neq x_i$ obtendo $v_i(x - x_i) = \gamma_i = 0$. Sendo A_i anéis de valorização próprios de $\mathbb{K}$, para $i \in \{1, \cdots, k\}$, e $A_1, \cdots, A_k$ dois a dois independentes, temos que $A_1, \cdots, A_k$ são incomparáveis. Portanto podemos utilizar o Teorema 3.3.1. Seja $R = A_1 \cap \cdots \cap A_k$ que é um anel de Prüfer, isto é, $\epsilon(R) = \beta(R)$. Como $\mathbb{K} \subseteq \beta(R) = \epsilon(R)$ vemos que $\mathbb{K} = R_M$ para algum sistema multiplicativo M de R. Portanto $\mathbb{K}$ é o corpo quociente para R e então $x_i = \tilde{d}_i c_i^{-1}$ com $\tilde{d}_i \in R$ e $c_i \in M$. Tomando $c = c_1 \cdots c_k$ e $d_i = \tilde{d}_i \cdot c_1 \cdots c_{i-1} c_{i+1} \cdots c_k$ temos que $x_i = d_i \cdot c^{-1}$. Seja $I_i = \{a \in m_{A_i}; v_i(a) > v_i(c) + \gamma_i\}$. Pelo Lema 3.3.2, I_i é um ideal próprio e não nulo de A_i. Segue da Proposição 3.3.3 que $C_i = I_i \cap R$ são ideais dois a dois comaximais de R. Desde que $d_1, \cdots, d_k \in R$, aplicamos o Teorema Chinês de Restos (Teorema 1.1.1) obtendo $d \in R$ tal que $(d - d_1, \cdots, d - d_k) \in C_1 \times \cdots \times C_k$. Tomando $x = \frac{d}{c}$ vem que $v_i(x - x_i) = v_i(dc^{-1} - d_i c^{-1}) = v_i(d - d_i) + v_i(c^{-1}) = v_i(d - d_i) - v_i(c) > v_i(c) + \gamma_i - v_i(c) = \gamma_i$. Note que d pode ser trocado por qualquer elemento do conjunto $d + C_1 \cdot C_2 \cdots C_k$. Assim temos uma infinidade de elementos $x \in \mathbb{K}$ tais que $v_i(x - x_i) > \gamma_i$. Escolhemos agora $y_i \in \mathbb{K}$ tal que $v_i(y_i) = \gamma_i$, e $y \in \mathbb{K}$ tal que $v_i(y - y_i) > \gamma_i$ para $i = \{1, \cdots, k\}$. Desde que $v_i(y_i) = \gamma_i < v_i(y - y_i)$ nós temos $v_i(y) = v_i((y - y_i) + y_i) = \gamma_i < v(x - x_i)$. Portanto $v_i(y + x - x_i) = \gamma_i$, isto é, todo elemento da forma $y + x$ satisfaz a condição desejada.

■

Corolário 3.3.2 *Sejam A_i, v_i e G_i como no Teorema. Dado $(\gamma_1, \cdots, \gamma_k) \in G_1 \times \cdots \times G_k$ existe uma infinidade de elementos $x \in \mathbb{K}$ tais que $v_i(x) = \gamma_i$, $i \in \{1, \cdots, k\}$.*

Referências Bibliográficas

[1] Artin, E. & Whaples, G. *Axiomatic Characterization of fields by the product formula for valuations.* Bull. Amer., Mathematical Society 51, 1945, 469 - 492.

[2] Atiyah, M. F. *Introduction al algebra commulativa.* Barcelona: Reverte, 1973.

[3] Bourbaki, N. *Elements of Mathematics.* Paris: Hermann, 1972.

[4] Dickson, L. E. *History of the Theory of Numbers.* New York, Chelsea, 1952.

[5] Domingues, H. H. *Espaços métricos e Introdução à Topologia.* São Paulo, Atual, 1982.

[6] Endler, O. *Teoria dos Números Algébricos.* Rio de Janeiro, Instituto de Matemática Pura e Aplicada, 1986.

[7] Endler, O. *Valuation Theory.* New York, Springer-Verlag, 1972.

[8] Faith, C. *Algebra II - Ring Theory.* New York, Springer-Verlag, 1976.

[9] Garcia, A. & Lequain, Y. *Álgebra: um curso de introdução.* Rio de Janeiro: IMPA, 1988.

[10] Gilmer, R. *Multiplicative ideal theory.* Marcel Dekker, 1972.

[11] Goldhaber, X. & Ehrlich, G. *Algebra.* London, The MacMillan Company, 1970.

[12] Gonçalves, A. *Introdução à álgebra.* Rio de Janeiro, Instituto de Matemática Pura e Aplicada, 1999.

[13] Gouvêa, F. Q. *Primeiros passos p-ádicos.* Notas do 17^0 Colóquio Brasileiro de Matemática, Rio de Janeiro, IMPA, 1989.

[14] Grosswald, E. *Topics from the Theory of Numbers.* Boston, Birkhäuser, 1984.

[15] Jenson, C.U. *Arithmetical Rings.* Acta Math. Acad. Sci. Hungar. 17, 115-123, 1966.

[16] Lang, S. *Algebra.* Amsterdan: Addison-Wesley, 1974.

[17] Larsen,M.D. & McCarthy, P.J. *Multiplicative theory of ideals.* Academic Press, 1971.

[18] LeVeque, W. J. *Topics in Number Theory - Vol. 1.* Massachussets, Addison Wesley, 1956.

[19] Lima, E. L. *Elementos de Topologia Geral.* Rio de Janeiro, Ao Livro Técnico S.A., 1970.

[20] Ostrowski, A. *Ostrowski, A. Untersuchungen zur Arithmetischen Theorie der Körper.* Math. Z. 39(1935), 369 - 404.

[21] Reiner, I. *Maximal Orders.* London, Academic Press, 1975.

[22] Samuel, P. *Algebraic Theory of Numbers.* Paris, Hermann, 1970.

[23] Tsu, S. *Suan-Ching (arithmetic).* edited by Y. Mikaini, Abhandlungen-Geschichte der Mathemetischen Wissenschaften 30 (1912), 32.

[24] Wieslaw W. *Topological Fields.* New York, Marcel Dekker, 1988.